Le protocole IP version 6 (IPv6)

Introduction

- Insuffisance des adresses IPv4 avec la croissance exponentielle du réseau Internet.
- Utilisation du CIDR et du NAT.
  En février 2011, le dernier bloc CIDR a été attribué !
  - Utilisation du protocole IPv6 qui remplacera bientôt IPv4.

Introduction

- IPv6 est déjà utilisé. Par exemple, certains FAI proposent une connexion IPv6.
- D'autres avantages à part l'adressage (tels que la suppression de la fragmentation au niveau des routeurs).

Taille d'une adresse IPv6

- Une adresse IPv6 tient sur 128 bits (16 octets ou encore 8 mots de 16 bits).
- On arrive alors à $2^{128} \approx 3{,}4 \times 10^{38}$ adresses.
- Image parlante : plus de 667 132 000 milliards d'adresses par un millimètre carré de la surface terrestre.
- Chaque machine peut disposer d'une adresse IPv6 publique (le NAT devient inutile).

RFC concernant l'adressage IPv6

- Une séquence de RFC intitulée « *IPv6 Addressing Architecture* »
  - RFC 1884 (décembre 1995)
  - RFC 2373 (juillet 1998)
  - RFC 3513 (avril 2003)
  - RFC 4291 (février 2006).
  - RFC 8200 (juillet 2017)

Types d’adresses IPv6

- Une adresse **unicast** désigne une seule interface. Un message envoyé à une adresse unicast est délivré à l'interface identifiée par cette adresse.
- Une adresse **anycast** désigne un ensemble d'interfaces. Un message envoyé à une adresse Anycats est délivré à l'interface la plus proche (selon le protocole de routage en question). Le type anycast n'existe pas en IPv4.
- Une adresse **multicast** désigne un ensemble d'interfaces. Un paquet envoyé à une adresse multicast est remis à toutes les interfaces que cette adresse désigne.

Types d’adresses IPv6

- Il n’existe pas d’adresse de broadcast en IPv6 : les fonctions correspondantes sont assurées par des adresses multicast.
- Une interface peut avoir plusieurs adresses IPv6 (unicast, anycast et multicast).

Représentation textuelles des adresses IPv6

- **Format complet :**
  - La forme est $x_1:x_2:x_3:x_4:x_5:x_6:x_7:x_8$ où chaque x_i est un mot de 16 bits exprimé en hexadécimal.
  - Il est permis d'omettre de 1 à 3 zéros (hexadécimaux) non significatifs dans chaque x_i : chaque x_i contient de 1 à 4 chiffres hexadécimaux.
- **Exemple**
  - 2007:0A8:9:0:0:75C:357:49C3 est une adresse IPv6 représentée dans le format complet.

Représentation textuelles des adresses IPv6

- **Format compressé**
  - Il est fréquent d'avoir des adresses IPv6 contenant de longues séquences de 0.
  - Pour alléger l'écriture, on a introduit le format compressé où une suite de zéro est remplacée par le mot « :: » qui ne doit apparaitre qu'une seule fois dans l'adresse pour pouvoir déduire la longueur d'une séquence de 0.

Représentation textuelles des adresses IPv6

- **Exemple**
  - Format complet. 2007 : A8 : 0 : 0 : 0 : 75C : 357 : 49C3
  - Format compressé. 2007 : A8 :: 75C : 357 : 49C3
  - Format complet. 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1
  - Format compressé. ::1

Représentation textuelles des adresses IPv6

- **Format mixte**
  - Plus convenable dans un environnement mixte (IPv4,IPv6)
  - La forme est : $x_1{:}x_2{:}x_3{:}x_4{:}x_5{:}x_6{:}d_1.d_2.d_3.d_4$ où $x_1{:}x_2{:}x_3{:}x_4{:}x_5{:}x_6$ représente les 6 mots de 16 bits de poids fort et $d_1.d_2.d_3.d_4$ représente 4 octets dans la notation décimale pointée du protocole IPv4.
  - Un exemple du format mixte est celui des adresses **IPv4- mapped IPv6.**

Représentation textuelles des adresses IPv6

- Une adresse IPv4-mapped IPv6 sert à représenter une adresse IPv4 sous forme d'une adresse IPv6.
- Le format d'une adresse IPv4-mapped IPv6 est $::ffff:d_1.d_2.d_3.d_4$ où $d_1.d_2.d_3.d_4$ est l'adresse IPv4 à mapper.
- **Exemple :** L'adresse IPv4-mapped IPv6 associée à l'adresse IPv4 139.124.187.4 est ::ffff:139.124.187.4

Adresses IPv6 particulières

- Adresse non spécifiée
  - Il s'agit de 0:0:0:0:0:0:0:0 ou :: en abrégé.
  - Cette adresse est généralement utilisée dans les sockets d'écoute (à toute adresse IPv6) ou dans les tables de routage.
  - Elle peut être aussi utilisée localement comme adresse source d'une machine qui n'a pas encore d'adresse.

Représentation textuelle canonique des adresses IPv6

- Avoir plusieurs représentations pour une même adresse IPv6 complique la recherche d'une adresse IPv6.
- Une recommandation pour une représentation textuelle canonique (unique) des adresses IPv6 a été proposée dans la RFC 5952 (août 2010).
- Cette représentation canonique est recommandée pour les systèmes qui doivent toutefois accepter et être capables de traiter toute représentation valide selon la RFC 4291.

Représentation des préfixes des adresses IPv6

- La représentation des préfixes des adresses IPv6 est similaire à celle en IPv4 avec la notation CIDR (Classless Inter-Domain Routing)
- Un préfixe est représenté par : **ipv6-address/ prefix-length**
- où prefix-length est une valeur décimale qui correspond aux nombre de bits les plus à gauche de l'adresse que contient le préfixe.
- Exemple : 2007:0AC8:0:CD30:0:0:0:0/60 représente le préfixe de 60 bits 20070AC80000CD3.

Représentation des préfixes des adresses IPv6

- L'adresse et le préfixe de l'adresse d'un noeud peuvent être combinés.
- Exemple :
  - Adresse du noeud : 2001:09DB:0:DD30:9753:3567:99AB:ABCD
  - Préfixe de son réseau : 2001:09DB:0:DD30::/60
  - Combinaison des deux : 2001:09DB:0:DD30:9753:3567:99AB:ABCD/60

URL et IPv6

- URL (Uniform Resource Locator) est une référence d'une ressource (par exemple, une page Web) sur Internet.
- Dans une URL, la machine sur laquelle se trouve la ressource peut être désignée par une adresse IPv4.
- Exemple : http://139.124.187.4/
  Pour spécifier le port, on rajoute “:” et le numéro du port Http://139.124.187.4:80

URL et IPv6

- Si on suit exactement le même principe en IPv6, on aura un problème d'ambiguïté.
- **Question** : http://100 : 37 : 29 : 145 ::15 : 80 indique :
  - http://100 : 37 : 29 : 145 : 0 :0 : 15 : 80 en utilisant le port par défaut ? ou bien
  - http://100 : 37 : 29 : 145 : 0 :0 : 0 :15 en utilisant le port 80 ?
  - **Solution** : une adresse IPv6 doit être mise entre crochets dans une URL
    - **http://[100 : 37 : 29 : 145 ::15] : 80**

Adresses Unicast

- Toute adresse unicast comprend une partie appelée ID interface qui sert à identifier l'interface dans un lien local.
- Toutes les adresses unicast (excepté celles qui commencent par 000 en binaire) doivent avoir un identifiant d'interface qui tient sur 64 bits.
- Deux méthodes pour générer automatiquement un ID d'interface :
  - **Selon le format EUI-64 modifié**
  - **Aléatoirement**

ID d'interface basé sur le format EUI-64 modifié

- L'ID d'interface basé sur le format EUI-64 modifié s'obtient à partir de l'adresse mac de l'interface en question en
  - injectant le bloc fffe au milieu de l'adresse mac (après le 3 ème octet)
  - modifiant le 7 ème bit (de gauche à droite).
  - **Exemple :** Soit une interface Ethernet ayant 84:2b:2b:a0:59:f7 comme adresse mac. L'ID d'interface basé sur le format EUI-64 modifié correspondant est 862b:2bff:fea0:59f7

Privacy extensions

- Utiliser une adresse IPv6 qui découle à partir de l'adresse mac permet d'identifier l'équipement utilisé et donc porte atteinte à la protection de la vie privée.
- Génération d'une valeur aléatoire et temporaire de l’identifiant ce qui garantit la confidentialité.

ID d'interface généré manuellement

- On peut aussi définir manuellement un ID d'interface.
- En général, pour les serveurs, il est plus facile de manipuler des adresses simples (par exemple : fe80::1).

Types d’adresses Unicast

- Il existe plusieurs types d'adresses IPv6 unicast :
  - Les adresses unicast globales
  - Les adresses unicast de lien local
  - Les adresses unicast de site local (déprécié)
  - Les adresses unicast locales uniques

Adresses unicast globales

- Portée globale (Internet)
- Le préfixe de routage désigne un site (un ensemble de sous-réseaux).
- L'ID de sous-réseau identifie un sous-réseau dans un site.

N bits	M bits	128-(N+M) bits
Préfixe de routage globale	Id. sous-réseau	Id. interface

Adresses unicast globales

- Toute adresse unicast globale qui ne commence pas par 000 en binaire se structure comme ci-dessous.
- Seul le bloc 2000 ::/3 (commençant par 001 en binaire) est ouvert actuellement à la délégation d'adresses unicast globales.
- **Exemple :** 2a00:1450:8007::6a est l'adresse IPv6 unicast globale associée à ipv6.google.com.

N bits	64-N bits	64 bits
Préfixe de routage globale	Id. sous-réseau	Id. interface

Adresse unicast de lien local

- La portée d'une adresse lien-local se limite au lien associé : aux interfaces directement connectées via un hub ou un switch (sans être obligé de passer par un routeur).
- Selon le RFC 4291, le bloc associé à ces adresses est fe80::/64.
- L'adresse est obtenue par concaténation du préfixe fe80::/64 avec l'ID d'interface ci-dessous
- Un hôte peut avoir plusieurs interfaces avec la même adresse de lien-local. L'ambiguïté est levée en précisant l'interface.

10 bits	54 bits	64 bits
1111111010	0	Id. interface

Adresse unicast en site local

- Les adresses unicast site-local ont été initialement conçues pour un adressage au sein d'un site sans avoir besoin d'un préfixe global.
- Ces adresses sont devenues obsolètes et leur préfixe doit être considéré comme un préfixe d'adresse unicast globale.

10 bits	54 bits	64 bits
1111111011	Id. sous-réseau	Id. interface

Adresses unicast locales uniques

- Ces adresses (définies dans la RFC 4193) sont dédiées à des communications locales tout en étant globalement uniques (avec une grande probabilité).
- Elles sont routables au sein d'une zone limitée : un site ou un ensemble limité de sites (mais pas sur Internet dans sa globalité).
- Ces adresses permettent d'interconnecter des sites privés sans créer des conflits d'adresses (car globalement “unique”) ou sans nécessiter aucune renumérotation.

Adresses unicast locales uniques

- Le préfixe associé est fc00::/7
- Le bit L vaut 1 actuellement (le préfixe est assigné localement). La signification de la valeur 0 pourrait être définie dans le futur.
- Le champ « Global ID » est générée aléatoirement. La partie « Subnet ID » correspond à l'ID d'un sous-réseau.

7 bits	1 bit	40 bits	16 bits	64 bits
1111110	L	Global ID.	Subnet ID.	Id. interface

Adresses multicast

- Une adresse multicast est structurée comme ci-dessous.
  - T = 0 indique une adresse multicast permanente qui est assignée par l'IANA (Internet Assigned Numbers Authority).
  - T = 1 indique une adresse multicast temporaire.
    Le champ portée désigne la portée du groupe multicast.

8 bits	4 bit	4 bits	112 bits
11111111	Flags (0 P R T)	Portée	Id. groupe

Adresses multicast

- Valeurs du champ portée:
  - 1 : interface local (utile pour les transmissions loopback)
  - 2 : lien local
  - 5 : site local
  - 8 : organisation locale (plusieurs sites appartenant à une même organisation)
  - E : global

Adresses multicast

- Une adresse multicast avec le préfixe ff02::/16 est une adresse multicast permanente d'un lien local.
- Une adresse multicast avec le préfixe ff15::/16 est une adresse multicast temporaire d'un site local.

Adresse multicast

- Une interface fait automatiquement partie du :
  - groupe ff02::1 comprenant tous les équipements présents sur le lien local (All-nodes group)
  - groupe dont l'adresse est l'adresse multicast sollicitée (solicited node address) de l'interface. Cette adresse est construite en ajoutant le préfixe ff02::1:ff00:0/104 aux 24 derniers bits de l'identifiant d'interface.
- **Exemple :** L'adresse multicast sollicitée correspondant à l'adresse 2037::01:800:200e:8c6c est ff02::1:ff0e:8c6c

Adresse multicast

- Les routeurs d'un segment IPv6 doivent appartenir au groupe all-routers désigné par ff02::2.

Adresses anycast

- Les adresses anycast sont prises du domaine des adresses unicast.
- Les adresses anycast sont utilisées par les routeurs (et non pas par les autres noeuds).

Les états successifs d'une adresse IPV6

- Chaque adresse IPv6 associée à une interface possède une durée de vie (qui peut être infinie) durant laquelle elle est dite valide.
- Quand la durée de vie expire, l'adresse devient invalide et peut être assignée à une autre interface.
- Afin de mieux gérer l'expiration de la durée de vie d'une adresse, cette dernière passe par deux états (préféré et déprécié) avant son expiration.

Les états successifs d'une adresse IPV6

- D'abord, une adresse se trouve dans un état préféré où il n'y a aucune restriction quant à son utilisation.
- Ensuite, elle passe à un état déprécié où les nouvelles communications devraient utiliser une autre adresse préférée (si c'est possible).
- L'adresse dépréciée reste utilisée par les communications qui l'ont déjà utilisée et qui n'arrivent pas à basculer vers une autre adresse.

Les états successifs d'une adresse IPV6

- Par défaut, les routeurs Cisco utilisent une durée de vie valide de 30 jours et une durée de vie préférée de 7 jours.
- Par défaut, une adresses de lien local a une durée de vie illimitée.

Les états successifs d'une adresse IPV6

- Pour garantir l'unicité des adresses IPv6 sur un lien, chaque noeud applique la procédure DAD (Duplicate Address Detection) avant toute attribution (manuelle ou automatique) d'une adresse IPv6 unicast à une interface.
- La procédure DAD doit être appliquée sur toutes les adresses (de lien local, locales uniques et globales) associées à une interface car actuellement elle ne sont pas forcément générées en utilisant le même identifiant d'interface.

Les états successifs d'une adresse IPV6

- Durant la procédure DAD, l'adresse est dite tentative et elle passe à l'état préféré dans le cas où la procédure DAD ne détecte pas d'adresse en double.
- Notons que le fait d'attribuer temporairement une adresse IPv6 à une interface permet de faciliter la renumérotation (changement d'adresse IP) : ceci évite de changer brusquement les adresses et interrompre les connexions qui sont en cours.
  - Tentative - Préférée - Dépréciée - Invalide

Datagramme IPv6

Datagramme IPv6

- Le processus de fragmentation/ré-assemblage au niveau des routeurs intermédiaires présent dans IPv4 n'existe plus dans IPv6 : si un routeur reçoit un paquet à transmettre à un réseau dont le MTU est inférieur à la taille du paquet, alors le routeur le supprime et envoie un message ICMPv6 de type **Packet Too** Big à la source du paquet.
- La fragmentation (si nécessaire) est assurée par la source du datagramme.
- Le but est de gagner en termes de performances.

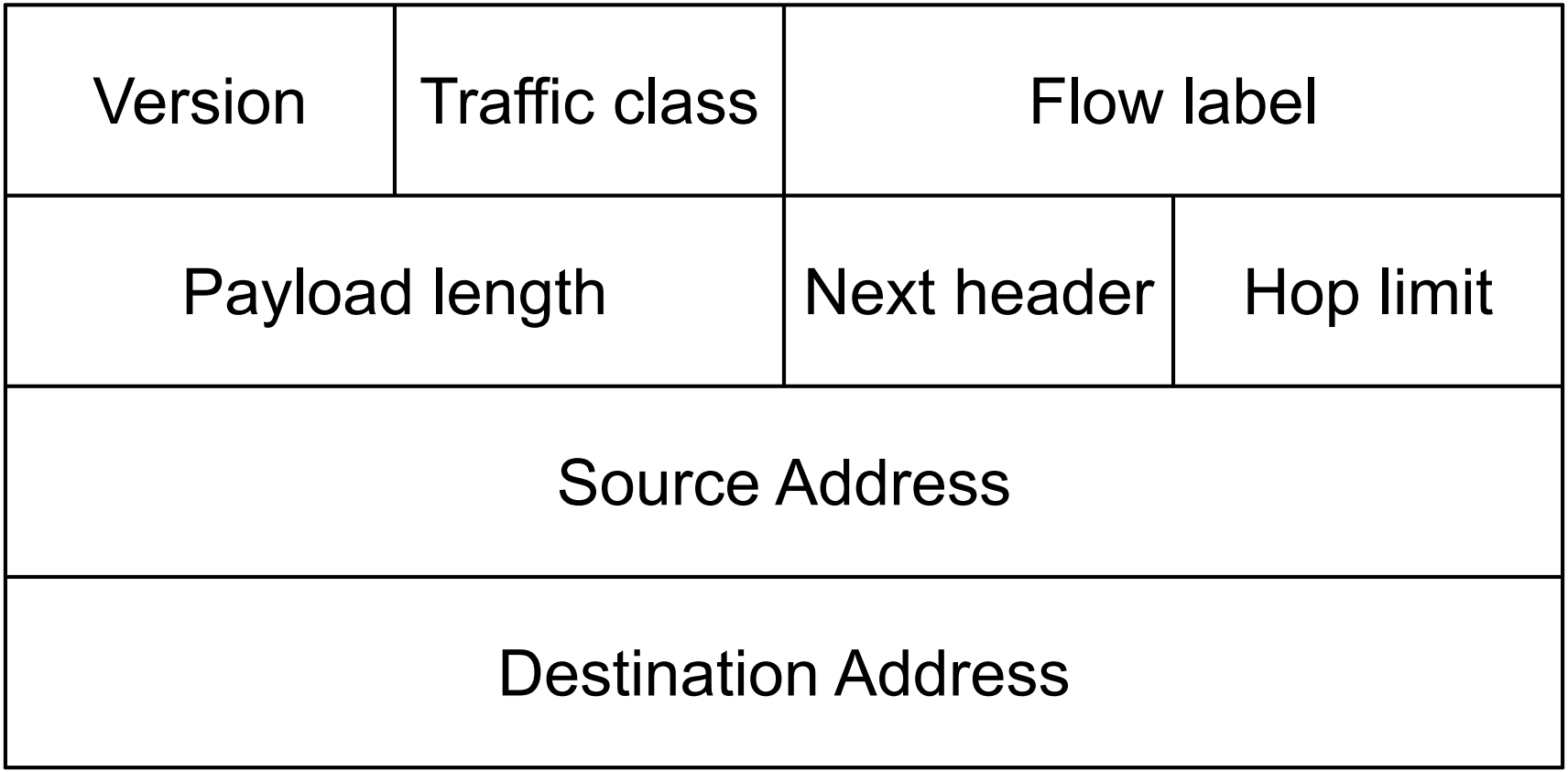
Datagramme IPv6

- Le cheksum dans IPv4 est recalculé par chaque routeur (car le TTL change).
- En IPv6, le checksum a été supprimé de l'entête.
- Pour éviter qu'un datagramme erroné, en particulier sur l'adresse de destination, ne se glisse dans une communication, tous les protocoles de niveau supérieur doivent utiliser un checksum qui prend en considération un pseudo entête comprenant les @ source et destination.

Datagramme IPv6

- Dans IPv6, le checksum est obligatoire pour UDP (alors qu'il est optionnel dans IPv4).
- Dans IPv6, le checksum d'ICMPv6 inclut le pseudo-entête (contrairement au checksum d'ICMP pour IPv4).
- Simplification du format de l'entête du datagramme IPv6 : certains champs IPv4 ont été supprimés ce qui permet de réduire le coût du traitement des paquets et aussi le coût de la bande passante.

Datagramme IPv6



Datagramme IPv6

- Version (4 bits) : version du protocol IP, elle vaut 6.
- Traffic Class (8 bits) : indique la priorité du datagramme (l'équivalent du ToS dans IPv4).
- Flow Label (20 bits) : une référence qui indique le flot (choisi par la source) auquel appartient le datagramme et donc elle indique le traitement associé qui doit être effectué par le routeur.
- Payload Length (16 bits) : taille du payload (charge utile), c-à-d la taille du datagramme moins l'entête (en octets).
- Next Header (8 bits) : le type d'entête qui suit immédiatement l'entête IPv6. Par exemple, ICMPv6(58), UDP (17), TCP(6), etc.
- Hop Limit (8 bits) : décrémenté de 1 à chaque fois que le datagramme passe par un routeur. Quand il atteint la valeur 0, le datagramme est détruit. Ce champ remplace le TTL (Time-to-Live) en IPv4.

Entêtes d’extension

- Les options du datagramme IPv4 ont été supprimées de l'entête IPv6.
- Elle sont remplacées par de nouvelles entêtes, dites entêtes d'extension, placées entre l'entête IPv6 et les données du datagramme.
  - La taille de l'entête IPv6 est fixe.
  - les entêtes d'extension peuvent être facilement ignorées par les routeurs intermédiaires.
- Notons que la plupart des extensions sont sensées être traitées uniquement par la sources et la (les) destination(s).

Entêtes d’extension

- Un packet IPv6 peut avoir zéro, une ou plusieurs entêtes, d'extension, chacune commence par un champ Next Header d'un octet qui définit le type de données qui suivent l'extension : une autre extension ou un protocole de niveau supérieur.
- Chaque entête d'extension est identifié par le champ Next Header de l'entête précédent.
- Exemple : Fragment header - 44

Taille d'un datagramme IPv6

- IPv6 requiert que chaque lien sur Internet ait un $MTU \geq 124$ (contre 64 octets pour IPv4).
- Pour un lien qui ne vérifie pas cette contrainte, des méthodes de fragmentation / ré-assemblage spécifiques doivent être fournies par une couche au dessous d'IPv6.

Path MTU Discovery

- Quand un noeud IPv6 a un message d'une taille importante à envoyer, il le transmet sous forme d'une série de datagrammes IPv6.
- L'idéal est que ces datagrammes aient la plus grande taille possible. Cette taille vaut le plus petit MTU sur le chemin entre la source et la destination.
- Le Path MTU est le plus petit MTU sur un chemin entre deux noeuds.

Path MTU Discovery

- Il est fortement recommandé que les noeuds IPv6 implantent le Path MTU Discovery (PMTUD) : une technique qui permet de trouver le Path MTU.
- L'application du PMTUD a pour but de découvrir et de tirer profit de Path MTU > la valeur minimale de 1280 octets.
- Les noeuds qui n'implantent pas le PMTUD se limitent à l'envoi de paquets qui ne dépassent pas 1280 octets ce qui conduit souvent à sous-exploiter les ressources réseaux car la plupart des chemins ont un Path MTU > 1280 octet.

Path MTU Discovery

- PMTUD supporte aussi bien les destinations unicast que les destinations multicast.
- Dans le cas d'un multicast, un paquet peut traverser plusieurs chemins pour arriver aux différentes destinations.
- On calcule alors le PMTU pour chacun de ces chemins, ensuite on prend le minimum.
- Le PMTUD peut être utilisé aussi dans IPv4 et dans ce cas le bit DF doit être positionné.

L’Algorithme Path MTU Discovery

- La source suppose que le PMTU = MTU du premier saut
- (étape *) Elle envoie le message avec cette hypothèse
- S'il existe un lien sur le chemin ayant un MTU inférieur à la taille du paquet alors le routeur en question détruit le paquet et envoie un message ICMPv6 de type Packet too big qui indique son MTU, soit MTU_R
  - La source met à jour PMTU = MTU_R
  - Revenir à (étape *)
- Le processus est réitéré jusqu'à ce que la source arrive à atteindre la destination.

Fragmentation au niveau de la source

- Pour envoyer un datagramme dont la taille dépasse le Path MTU, il est possible de le fragmenter au niveau de la source et de mettre chaque fragment dans un datagramme.
- Ces datagrammes doivent être ré-assemblés par le récepteur.
- La fragmentation est déconseillée quand il est possible d'ajuster les paquets en fonction du Path MTU !
- Les paquets issus de la fragmentation contiennent un entête d'extension : entête de fragmentation.

Next header	Reserved	Fragment offset	Res	M
Identification				

Entête de fragmentation

- Next Header (8 bits) : identifie le type du premier entête de la partie fragmentable du message original.
- Reserved (8 bits) : Il est prévu pour des besoins futurs. Entre temps, il vaut 0 pour l'émission et doit être ignoré pour la réception.
- Fragment Offset (13 bits) : le déplacement, en 8 octets, des données qui suivent cette entête par rapport au début de la partie fragmentable du paquet initial. La taille (en octet) de chaque fragment (à part le dernier) doit être multiple de 8.
- Res (2 bits) : initialisé à 0 pour l'émission et ignoré à la réception.
  M (1 bit) :
  - M = 1 : more fragments
  - M = 0 : dernier fragment.
- Identification (32 bits) : Pour chaque paquet à fragmenter, la source génère un identificateur.

ICMPv6

ICMPv6 (RFC 4443)

- IP (v4 ou v6) n'est pas fiable
  - ICMP (v4 ou v6) est un module obligatoire pour IP.
- ICMPv6 assure les fonctionnalités de :
  - ICMP dans IPv4 (rapporter des erreurs et effectuer des diagnostics).
  - ARP (Address Resolution Protocol) dans IPv4 permettant de découvrir le voisinage.
  - IGMP (Internet Group Member Ship Protocol) dans IPv4 permettant l'inscription ou l'abonnement à un groupe multicast.
- Un message ICMPv6 s'encapsule dans un datagramme IPv6 où le champ Next Header vaut 58.

ICMPv6

- Type (8 bits) : type du message, sa valeur détermine le format des données restantes.
- Code (8 bits) : dépend du type, ça permet de préciser le type
- Checksum (16 bits) : permet de détecter des erreurs dans le message ICMPv6 et certaines parties de l'entête IPv6.
- Les messages ICMPv6 (32 bits) peuvent être regroupées dans deux familles : messages d'erreurs et message d'information.

Type	Code	Checksum
Message body		

Checksum ICMPv6

- Le checksum se calcule en fonction de tout le message ICMPv6 (avec checksum initialisé à 0) préfixé par le pseudo entête IPv6 où Next Header vaut 58.
- ICMPv6 inclut le pseudo entête dans le calcul du checksum et ce contrairement à ICMP dans IPv4.
- L'objectif est de vérifier l'intégrité des champs du pseudo entête desquels dépend le message ICMPv6 et qui ne sont pas couverts par un checksum de l'entête IPv6 à l'inverse d'IPv4.

Checksum ICMPv6
Pseudo entête

<table>
<tr><td colspan="2">Adresse source</td></tr>
<tr><td colspan="2">Adresse destination</td></tr>
<tr><td colspan="2">longueur du paquet de la couche supérieure</td></tr>
<tr><td>Zéro</td><td>Next header = 58</td></tr>
</table>

Messages d’erreurs

- Le type est dans [0, 127]
- **Exemple :**
  - 1 Destination Unreachable
  - 2 Packet Too Big
  - 3 Time Exceeded
  - etc.

Message d’information

- Le type est dans [128, 255]
- Exemple
  - 128 Echo Request
  - 129 Echo Reply
  - ...

Destination unreachable

- Type = 1
- Code = 0 : Pas de route vers la destination
- Code = 1 : La communication avec la destination est administrativement interdite
- Code = 2 : La destination est au delà de la portée de l'adresse source. Par exemple, un paquet ayant une adresse source de lien local et une adresse de destination globale.
- Code = 3 : Address inaccessible : utilisé quand le problème ne correspond à aucun des problèmes précédents.
  Par exemple : impossibilité de résoudre l'adresse IPv6 de la destination en une adresse de liaison.
- Code = 4 : Port inaccessible
- Code = 5 : Interdiction par une politique de sécurité.
- Code = 6 : La route vers la destination est une route reject. Les codes 5 et 6 précisent le code 1.

Packet too big

- Un message Packet too big doit être envoyé par un routeur lorsqu'il reçoit un paquet qu'il ne peut pas acheminer car sa taille est plus grande que le MTU du lien suivant.
- Type : 2
- Code : initialisé à 0 par l'émetteur et ignoré par le récepteur (tout comme le champ unused du message destination unreachable).
- MTU : le MTU du lien suivant.
  Ce message est utilisé par le PMTUD.

Découverte du voisinage (RFC 4861)

- Les noeuds IPv6 utilisent le protocole NDP (Neighbor Discovery Protocol) pour :
  - obtenir l'adresse physique d'un voisin qui se trouve sur le même lien (fonction de résolution d'adresse assurée par ARP dans IPv4) et aussi pour communiquer à ce voisin son adresse physique
  - pour découvrir les routeurs et obtenir éventuellement une (des) adresse(s) globale(s), etc.
- NDP utilise les cinq messages ICMPv6 suivants :
  - Type 133 : RS
  - Type 134 : RA
  - Type 135 : NS
  - Type 136 : NA
  - Type 137 : Router redirect

Découverte du voisinage (RFC 4861)

- Pour ces cinq messages, le champ Hop Limit est initialisé par l'émetteur à la valeur maximale de **255**.
- Les paquets NDP reçus doivent avoir cette valeur de Hop Limit. Sinon, il s'agit de messages de découverte de voisinage qui proviennent de l'extérieur du lien.
- Code vaut zéro pour tous les cinq messages.
- Les messages NDP comprennent zéro, une ou plusieurs options qui commencent toutes par un type et une longueur dont l'unité est de 64 bits.

Message RS

- Type = 133
- Code = 0
- Reserved : initialisé à 0 par l'émetteur et ignoré par le récepteur
- Si l'adresse IPv6 source est différente de l'adresse non spécifiée alors, on a l'option “Source link-layer address” dont le type vaut 1.

Message RA

- Type = 134, code = 0
- Un routeur émet périodiquement un message d'annonce de routeur **RA (Router Advertisement)** mais il peut également l'émettre en réponse à une sollicitation de routeur RS.
- Dans l'en-tête IPv6, l'adresse source est l'adresse lien-local de l'interface du routeur qui émet le message RA.
- L'adresse destination est celle de l'équipement qui a sollicité le routeur ou l'adresse multicast ff02 ::1 du groupe de «Tous les nœuds » sur un lien local.

Message RA

- Cur Hop Limit : la valeur par défaut qui doit être placée dans le champ Hop Limit de l'entête IP des paquets sortants. Une valeur nulle veut dire que ce champ n'est pas spécifié par ce routeur.
- M : “Managed address configuration" flag.
  M = 1 : des adresses sont disponibles via DHCPv6.
- O : "Other stateful configuration" flag.
  O = 1 => d'autres informations de configuration (telles que celles liées au DNS) sont disponibles via DHCPv6.
- Quand le flag M est positionné, le DHCPv6 retourne toutes les informations de configuration et donc le flag O peut être ignoré car redondant.

Message RA

- Router life time : indique le temps en secondes durant lequel le routeur qui fait l'annonce jouera le rôle du routeur par défaut. La valeur maximale est de 65535 secondes.
- Reachable Time : le temps, en millisecondes, pendant lequel un noeud suppose qu'un voisin est joignable après avoir reçu une confirmation d'accessibilité.
- Retrans Timer : le délai (en millisecondes) pour retransmettre un message NS. Utilisé par exemple dans la procédure DAD. La valeur zero veut dire que ce paramètre n'est pas spécifié par le routeur.

Message RA

- Options possibles
  - Source link-layer address (type 1) qui correspond à l'adresse physique de l'interface du routeur à partir de laquelle le message RA a été émis.
  - MTU (type 5).
  - Prefix information (type 3) : ces options spécifient tous les préfixes utilisés pour l’auto-configuration sans état.

Message RA

- Length : 4 (4 * 64 bits)
- Prefix Length (8 bits) : la taille du préfixe
- L (on-Link) à 1 indique que tous les équipements partageant ce préfixe, partagent également le même lien et sont donc directement accessibles. Sinon, on ne peut rien déduire.
- A (Autonomous) à 1 indique que le préfixe annoncé peut être utilisé dans l'auto-configuration sans état.
- Valid (resp. Preferred) lifetime (32 bits): indique la durée de vie valide (resp. préférée) en sec de l'adresse générée en utilisant ce préfixe. La valeur 0Xffffffff indique l'infini.
- Le préfixe annoncé est placé dans un champ de 128 bit. Un routeur ne devrait pas envoyer un préfixe associé au lien local.

Message NS

- Un noeud envoie un message de sollicitation de voisin NS (Neighbor Solicitation) afin d'obtenir l'adresse physique d'un noeud tout en lui communiquant sa propre adresse physique. Le message NS est envoyé vers l'adresse multicast sollicitée associée à la cible.
- Un message NS peut être également utilisé afin de vérifier l'accessibilité d'un voisin et dans ce cas il est envoyé en unicast.
- L'adresse source de l'entête IPv6 correspond à l'adresse de l'interface ayant envoyé le message sinon il s'agit de l'adresse non spécifiée :: (le processus DAD est en cours).

Message NS

- Type = 135
  - Target Address : l'adresse objet de la requête
    Possibilité d'avoir l'option “ Source link-layer address” telle que :
    - l'option ne doit pas être incluse quand l'adresse source de l'en-tête IPv6 est l'adresse non spécifiée
    - l'option doit être incluse quand l'interface dispose d'une adresse IPv6 et quand le message est destiné à l'adresse multicast.
    - l'option peut être incluse lorsque le message est envoyé à l'adresse unicast (vérification de l'accessibilité du voisin).

Message NA

- Un message d'annonce de voisin NA (pour Neighbor Advertisement) est émis en réponse à un message de sollicitation de voisin : annonce sollicitée.
- Il peut aussi être émis pour indiquer un changement d'une correspondance (adr physique, adr IP) : annonce non sollicitée.
- Dans l'en-tête IPv6, l'adresse source est une adresse de l'interface qui émet l'annonce.
- Adresse de destination :
  - annonces non sollicitées : typiquement, l'adresse multicast de tous les noeuds ff02::1
  - annonces sollicitées, si l'adresse source du message de sollicitation a été spécifiée, alors c'est cette adresse. Sinon, c'est ff02::1.

Message NA

- Type = 136
  - R (Router flag) : quand il est positionné, il indique que l'émetteur est un routeur.
  - S (Solicited flag) : quand il est positionné, il s'agit d'une annonce sollicitée.
  - O (Override flag) : quand il est positionné, il indique que l’annonce peut mettre à jour une entrée dans le cache de correspondance (adresse physique, adresse IP) des stations qui reçoivent le message. Sinon, seuls les ajouts dans la table sont autorisés.

Message NA

- Target address :
  - Pour les annonces sollicitées, il s'agit de l'adresse de la cible du message de sollicitation : adresse IPv6 objet de la requête.
  - Pour une annonce non sollicitée, il s'agit de l'adresse IPv6 dont l'adresse physique a changé.
- Options possibles :
  - Target link layer address (de type 2) : l'adresse physique de l'émetteur de l'annonce. Elle doit être incluse pour les sollicitations multicast. Pour les sollicitations unicast, elle peut être supprimée car l'émetteur de la sollicitation connait déjà l'adresse physique.

Auto-configuration d'adresse sans état

Introduction

- Le processus d'auto-configuration comprend :
  - la génération d'une adresse de lien-local
  - la génération d'adresses globales ou uniques locales (cette étape ne concerne pas les routeurs)
  - la procédure DAD (Duplicate Address Detection) pour la détection d'adresses en double sur un même lien

Introduction

- Deux types d'auto-configuration :
  - Sans état (ou stateless auto-configuaration)
  - DHCPv6 (pour avoir un contrôle plus strict sur l'affectation des adresses).

Introduction

- L'auto-configuration sans état permet à un hôte de générer ses adresses (globales et uniques locales) en combinant l'ID interface qu'il génère lui même et le(s) préfixe(s) annoncé(s) périodiquement par le routeur associé.
- Elle ne nécessite aucun serveur en plus.
- En l'absence d'un routeur, les adresses de lien-local sont suffisantes pour communiquer avec les noeuds du même lien.

Génération d’une adresse lien-local

- Dans l'auto-configuration sans état, un noeud génère une adresse de lien-local après l'un des évènements suivants :
  - Initialisation d'une interface au démarrage du système
  - Ré-initialisation d'une interface après sa désactivation
  - Suite à un premier rattachement d'une interface à un lien
- Une adresse lien-local est formée en combinant l'ID d'interface et le préfixe de lien-local fe80::/64

DAD

- La procédure DAD utilise des messages ICMPv6 de type **NS** (pour **Neighbor Solicitation**)
- Un noeud envoie un certain nombre de messages NS.
- Ce nombre est représenté par la variable DupAddrDetectTransmit qui vaut 1 par défaut.
- Le délai entre deux messages NS consécutifs est RetransTimer millesecondes.
- C'est aussi le délai entre l'envoie du dernier NS et la fin de la procédure DAD.

DAD

- Une adresse est considérée comme étant unique si on ne détecte aucune duplication au bout de RetransTimer millesecondes après l'envoi de DupAddrDetectTransmits messages NS.
- Avant d'envoyer un message NS, l'interface doit joindre :
  - le groupe multicast all-nodes
  - le groupe multicast sollicité associé à l'adresse tentative.

DAD

- L'adresse IP source (pour envoyer le message NS) est l'adresse non spécifiée ::
- L'adresse IP destination (pour envoyer le message NS) est l'adresse multicast **sollicitée** associée à l'adresse tentative.
- Le message NS contient l'adresse tentative (dont la vérification d'unicité est en cours) dans un champ appelé “**address target**”.

DAD

- S'il existe un noeud qui possède la même adresse que l'adresse tentative, alors ce dernier répond par un message NA (Neighbor Advertisement) qu'il envoie au groupe all-nodes : l'adresse tentative ne sera pas affectée au noeud appliquant le DAD.
- Si le noeud (qui a envoyé le NS) reçoit un message de sollicitation NS (à part le sien éventuellement) pour la même adresse pendant la procédure DAD, on déduit qu'il existe un autre noeud qui applique le DAD relativement à la même adresse.
- Cette dernière ne sera assignée à aucun des deux noeuds.
- Sinon, l'adresse est unique.

Génération d’adresses globales

- Les routeurs émettent périodiquement des messages ICMPv6 de type **RA (Router Advertissement)** vers le groupe all-nodes.
- Un message RA contient le(s) préfixe(s) utilisé(s) pour les adresses globales.
- Afin d'obtenir un message RA rapidement, un hôte émet un message **RS (Router Sollicitation).**
- Si un hôte envoie 3 messages RS et ne reçoit aucun message RA au bout d'une seconde après l'envoie du 3ème message RS, alors il déduit qu'il n'existe aucun routeur sur son lien.

Sources

- Safa Yahi, IPv6 : parties 1 et 2, supports de cours, 2011.