Réseaux et Systèmes (MIN 15112)

2025 - 2026

Zhiyi Zhang

zhiyi.zhang@uvsq.fr

https://www.zhiyizhang.com

UVSQ

université PARIS-SACLAY

NAT
(Network Address Translation)

Rappel : classes d'adresses IPv4

	8 bits	8 bits	8 bits	8 bits
A	0xxxxxxx	Hôte	Hôte	Hôte
B	10xxxxxx	Réseau	Hôte	Hôte
C	110xxxxx	Réseau	Réseau	Hôte
D	1110xxxx	Multicast	Multicast	Multicast
E	Réservé			

Contexte

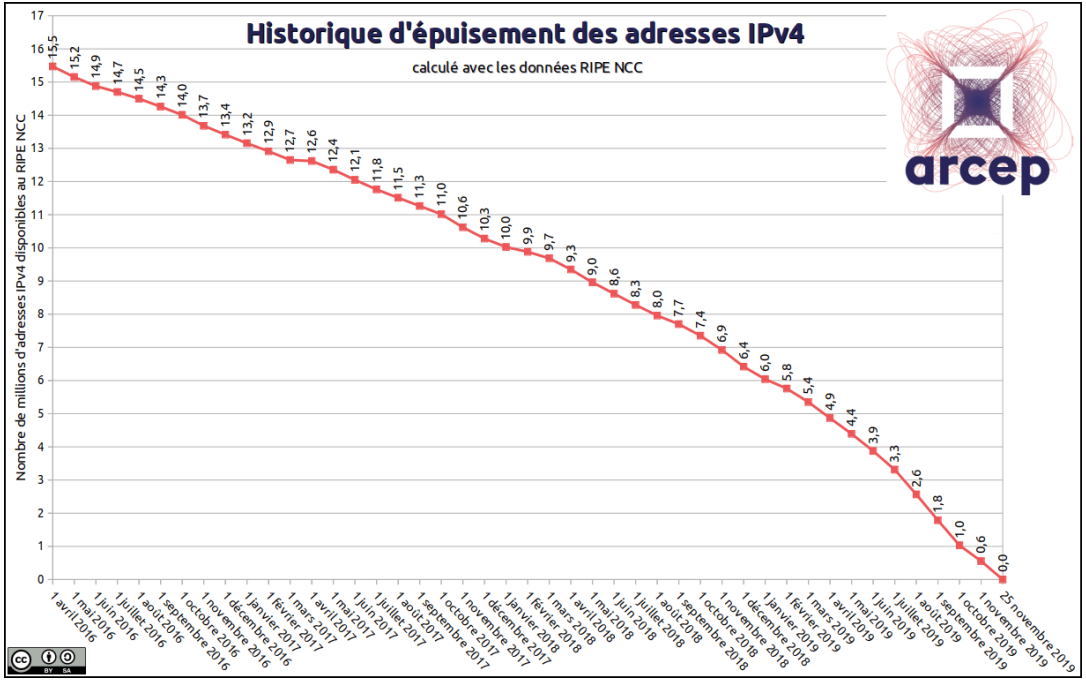
Épuisement des adresses IPv4

Solutions :

DHCP

IPv6

NAT



Adresses publiques

Adresse publique :

Une adresse utilisée sur Internet et unique au niveau mondial.

- Unique sur tout Internet
- Permet une communication directe avec d'autres machines sur Internet
- Attribuée par des organismes officiels
- Utilisée pour les routeurs d'accès Internet, serveurs, sites web …

Adresse privée

Adresse privée :

Une adresse utilisée uniquement dans les réseaux locaux.

- Non unique (réutilisable dans différents réseaux)
- Ne peut pas accéder directement à Internet
- Gratuit, pas besoin d’enregistrer

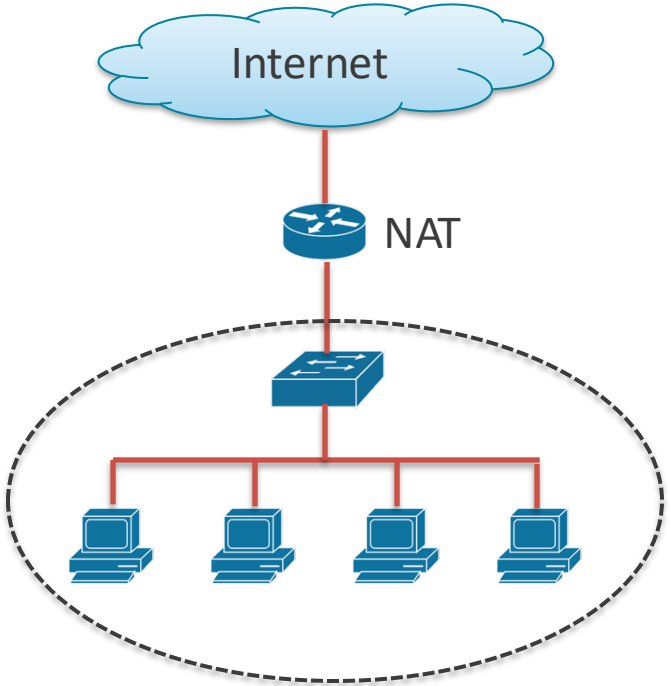
NAT

NAT (Network Address Translation)

RFC 3022

Rôle du NAT :

- Convertit les adresses privées -> adresse publique
- Permet à plusieurs machines de partager une seule adresse publique



Plage d’adresses privées

- 10.0.0.0/8, hôte : 24 bits
  10.0.0.0 à 10.255.255.255

- 172.16.0.0/12, hôte : 20 bits
  172.16.0.0 à 172.31.255.255

- 192.168.0.0/16, hôte : 16 bits
  192.168.0.0 à 192.168.255.255

NAT

Adresses NAT

- Adresse locale interne (Inside Local Address)
  L'adresse d'un hôte interne, souvent une adresse privée
- Adresse globale interne (Inside Global Address)
  L'adresse publique attribuée à l'hôte interne par le routeur NAT
- Adresse globale externe (Outside Global Address)
  L'adresse réelle et publique de l'hôte externe sur Internet
- Adresse locale externe (Outside Local Address)
  L'adresse d'un hôte externe, souvent identique à l'adresse globale externe

NAT

Adresse interne

Adresse externe

NAT statique

NAT statique : mappage **permanent** 1 à 1

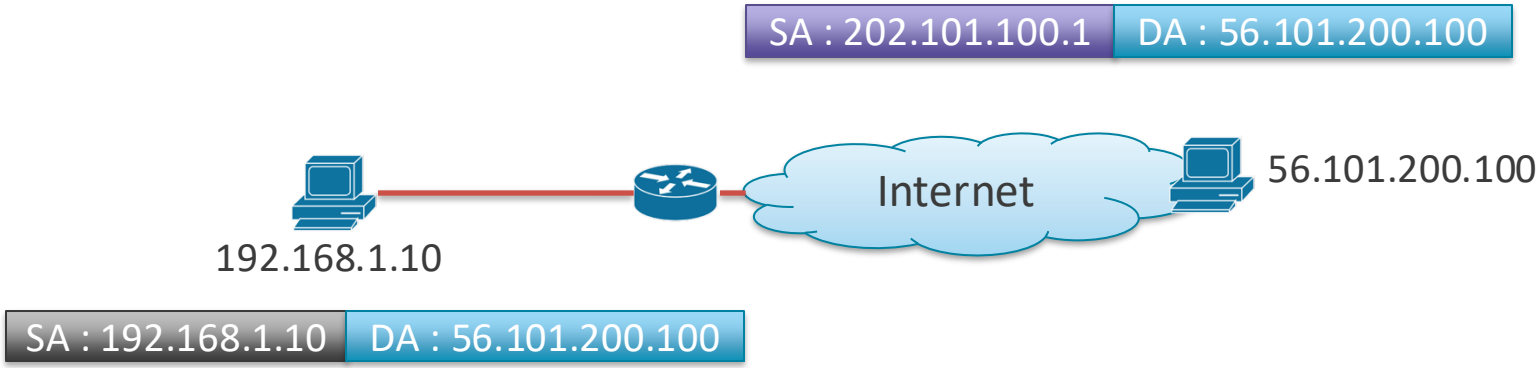
Utilisé lorsqu'une machine interne doit être accessible depuis Internet (serveur, caméra …)

- Une adresse privée – une adresse publique
- Correspondance fixe, le mappage ne change jamais

Cons :

- Consomme une adresse publique par machine
- Pas de gain d'adresses

NAT statique



Adresse locale interne	Adresse globale interne
192.168.1.10	202.101.100.1

NAT dynamique

NAT dynamique : mappage dynamique 1 à 1

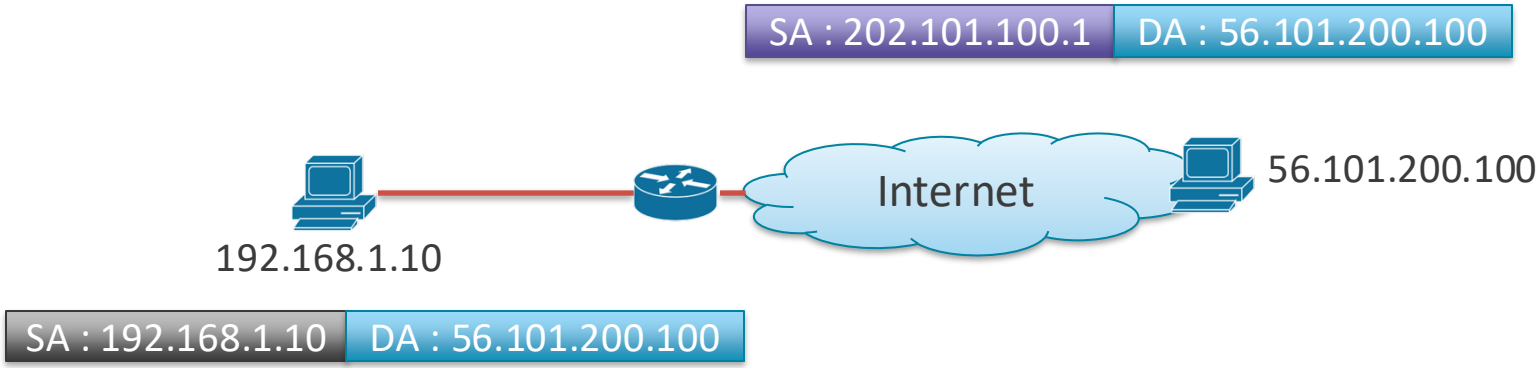
Traduire des adresses privées en adresses publique à partir d'un **pool d'adresse**.

La correspondance n'est pas fixe, l'hôte internet reçoit une adresse publique **temporairement**. Une fois la communication terminée, l'adresse publique est **libérée**.

Cons :

- Une session peut échouer si le pool est plein

NAT dynamique



ip nat pool xx 202.101.100.1 - 10

Adresse locale interne	Adresse globale interne
192.168.1.10	202.101.100.1

PAT

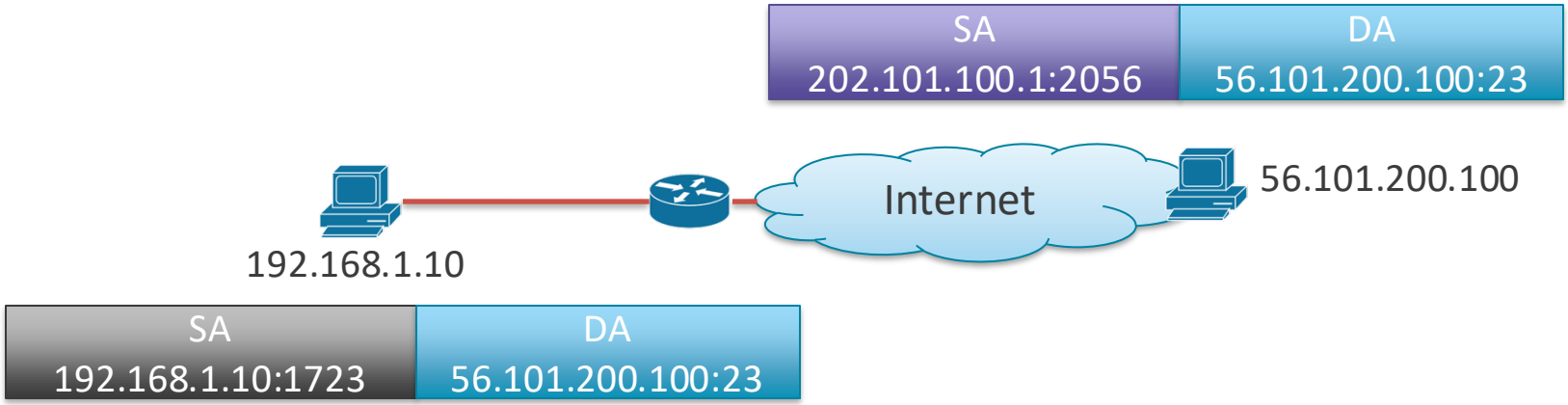
PAT (Port Address Translation) : N à 1

PAT permet à plusieurs hôtes internes de partager une seule adresse publique en utilisant des numéros de port différents.

Cons :

- Pas adapté aux services qui doivent être accessible depuis l'extérieur, sauf si on configure une redirection de port.
- En théorie, le nombre de ports disponibles peut être saturé.

PAT



Adresse locale interne	Adresse globale interne	Adresse globale externe
192.168.1.10:1723	202.101.100.1:2056	56.101.200.100:23

UVSQ

université PARIS-SACLAY

IPv6

Pourquoi une nouvelle version ?

- Pénurie d’adresses IPv4
- La taille des tables de routage des routeurs cœur de l’Internet explosent
- Supprimer les mauvaises solutions d’urgence (NAT)

NAT IPv4

Une seule adresse publique représente toutes les adresses privées

Pro : Confidentialité des adresses privées

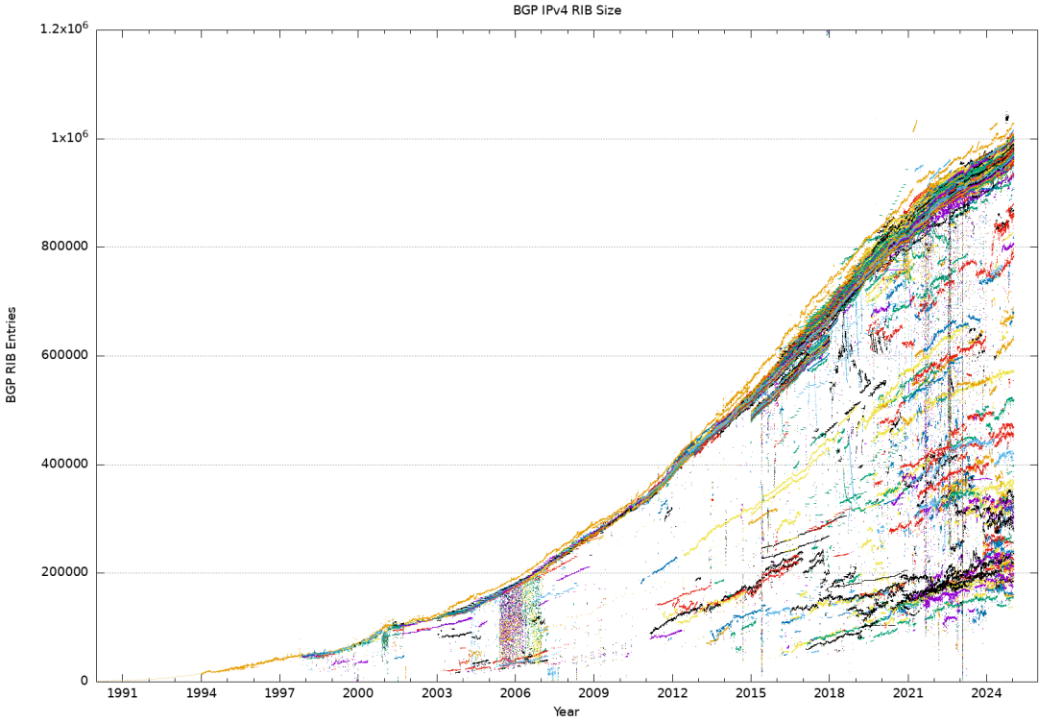
Cons :

- Conflits d'adressage privé lors de la fusion de réseaux
- Manipulation des entêtes -> sécurité de bout en bout impossible (intégrité)
- Bottleneck de performance :
  Chaque paquet est modifié par le routeur NAT
  Le routeur NAT doit conserver une entrée pour chaque connexion active

Taille de Table de routage au cœur de Internet

UVSQ université PARIS-SACLAY

>10^6 entrées



Source : cidr-report.org

Adressage IPv6

Adresse plus longue : 128 bits

Théoriquement, 2^{128} adresses

- Adressage globale hiérarchique
- Trois types d'adresse globales
  Unicast
  Multicast
  Anycast
- Une interface peut avoir plusieurs adresses IPv6
- Plus de broadcast en IPv6

Format adresses IPv6

Format des adresses IPv6

RFC 4291 / 3587

Préfixe : on note @IPv6/taille de préfixe, plus de masque de sous-réseau

Interface identifier :

- paramétré manuellement
- généré aléatoirement selon des mécanismes de cryptage (privacy, *RFC 8981*)
- généré automatiquement sur la base de l'adresse MAC IEEE 802 (mécanisme EUI-64)

Adresse IPv6

Exemple : 2001:0000:0000:0000:0003:F8FF:FE21:67CF/64

- Notation canonique **hexadécimale** en **8 blocs de 16 bits et chaque bloc comprend lui-même 4 mots de 4 bits**
- Au début de chaque bloc, on peut supprimer de 1 à 3 « 0 ».
  Exemple : 2001:0:0:0:3:F8FF:FE21:67CF/64
- Les blocs successifs de « 0000 » peuvent être remplacés par « :: » (une seule fois pour éviter toute ambiguïté)
  Notation équivalente : 2001::3:F8FF:FE21:67CF/64
- Préfixe réseau 2001::/64 (4 blocs de 16 bits)
  Identifiant interface 0003:F8FF:FE21:67CF (4 blocs de 16 bits)

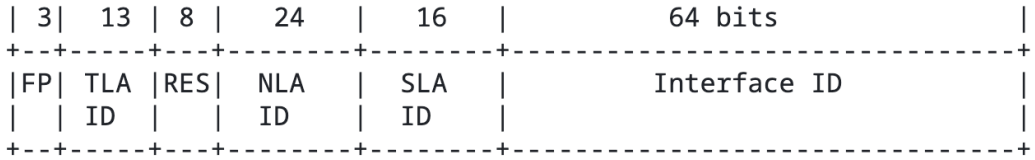
Type d’adresses IPv6

- Adresse unicast
  Un paquet envoyé sera traité par une seule interface

- Adresse anycast
  Un paquet envoyé sera traité par une seule interface d’un groupe, la plus proche en termes de routage

- Adresse multicast
  Un paquet envoyé sera traité par un groupe d’interfaces

Adresse unicast globale (*RFC 2374*)



FP : Format prefix (001 pour unicast globale; 010 pour tests)

TLA ID (Top Level Aggregator) : identifie un organisme public gérant un réseau public tel que l'IANA (Internet Assigned Numbers Authority) ou les RIR (Regional Internet Registry)

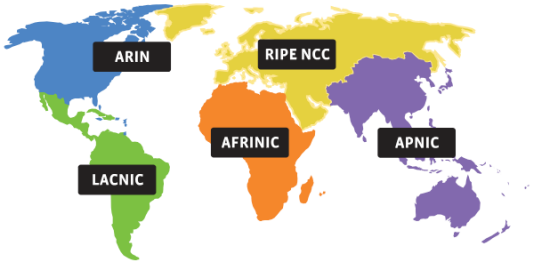
RES : Réservé pour étendre les champs TLD/NLA

NLA ID (Next Level Aggregator) : identifie un opérateur réseau

SLA ID (Site Level Aggregator) : identifie les sous-réseaux au sein d'un site

Top Level Aggregator

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia



Source : https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

L'allocation des adresses unicast globale aux TLA

Adresses unicast particulières

- Adresse lien-local (Link-Local unicast)
  FE80::Interface ID/10
  L'adresse lien-local est valable uniquement sur le lien local (même réseau)
  Non-routable au-delà du lien local !

- Adresse unique locale (Unique local address)
  FC00::Interface ID/7
  L'adresse ULA (unique local address) est utilisée à **l'intérieur d'un réseau privé**.
  En pratique, on utilise FD00::/8 avec Global ID (40 bits) : généré aléatoirement
  Une ULA utilise donc un préfixe /48

Adresse multicast

Flags : 000T
T=0 : multicast permanente
T=1 : multicast temporaire

Scope
1 : Interface-local
2 : Link-local
4 : Admin-local
5 : Site-local
8 : Org-local
E : Global

Groupes multicast particuliers :
FF02::1 -> Toutes les stations IPv6
FF02::2 -> Tous les routeurs IPv6

Plus de détails : https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

Adresse anycast

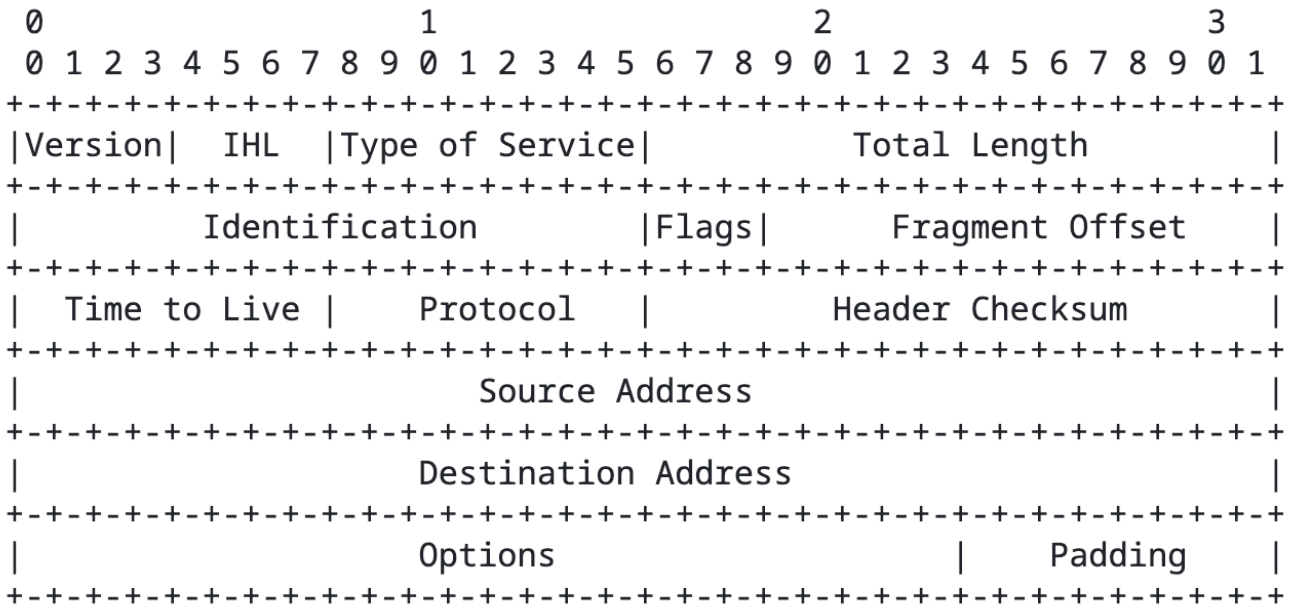
- Même adresse attribuée à plus d'une interface sur des nœuds différents.
- Paquet est routé vers l'interface *la plus proche,* au sens du routage
- Usage : interrogation des serveurs, DNS, DHCP …
- Uniquement adresses de destination

Adresses particulières

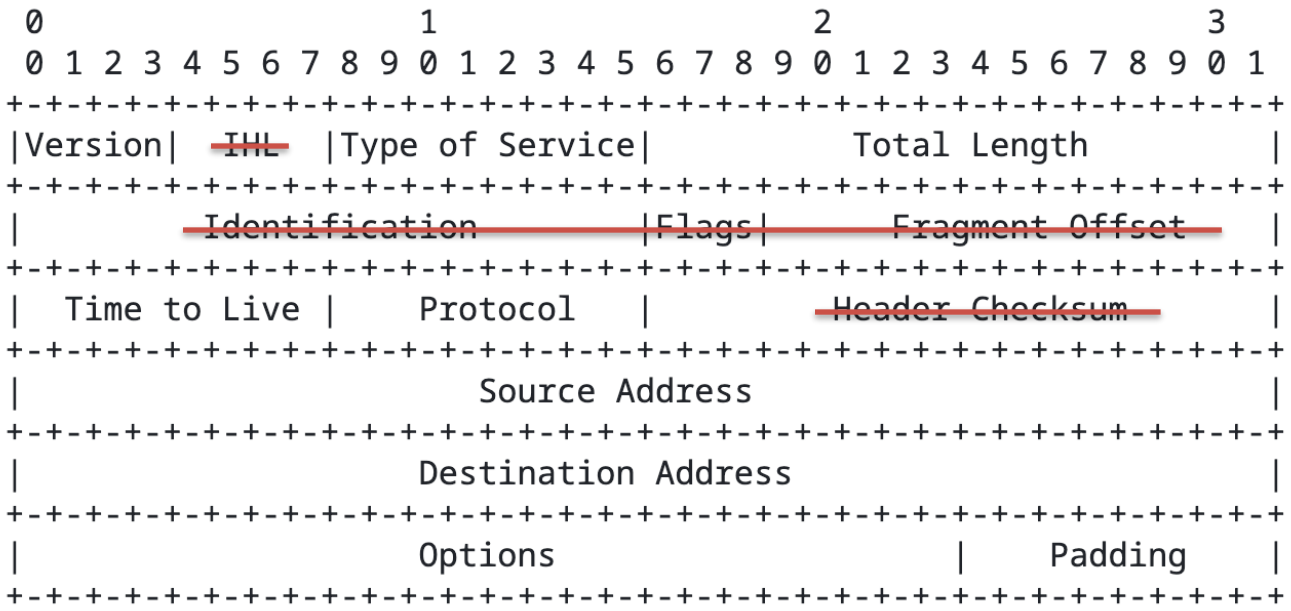
- Loopback
  0:0:0:0:0:0:0:1/128 ou ::1/128
  équivalent adresse IPv4 : 127.0.0.1

- Adresse non spécifiée
  0:0:0:0:0:0:0:0/128 ou ::/128
  Ne peut jamais être adresse de destination
  Peut être utilisée comme adresse source (exemple : DHCP)

Rappel : en-tête IPv4 (*RFC 791*)



IPv4 -> IPv6


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

IPv4 -> IPv6

Champs conservés :

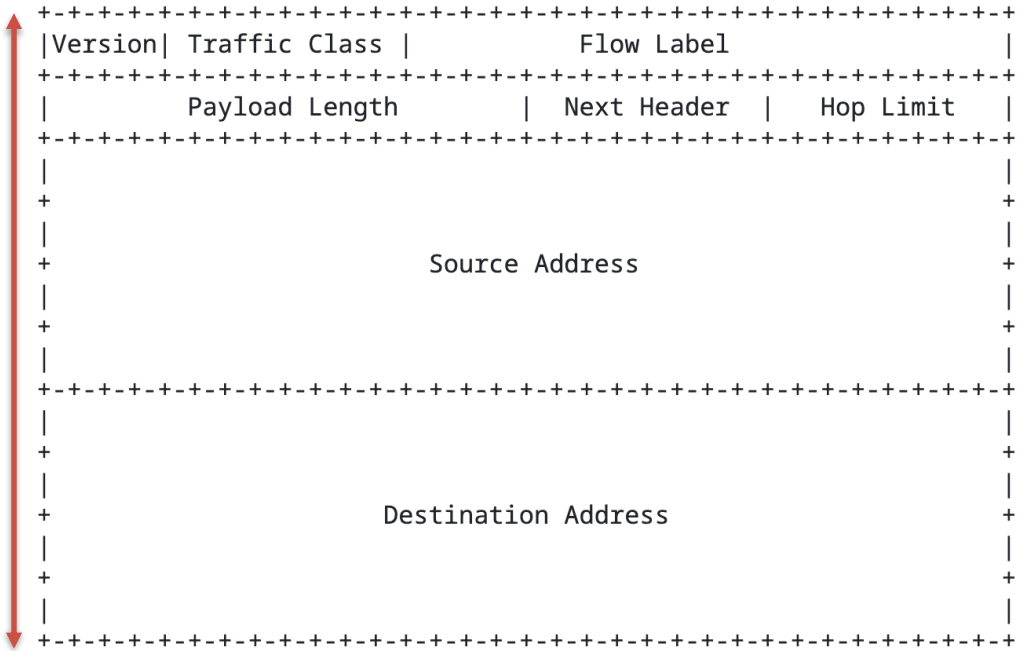
- Version
- ToS (Type of Service) – Traffic class
- Total length – Payload length
- Protocol type – Next header
- TTL (Time to Live) – Hop limit

Champ rajouté : Flow label

Pas d’options, remplacées par les en-têtes d’extension

En-tête IPv6

40 octets



En-tête IPv6

Version (4 bits)

Traffic Class (8 bits) : Priorités ou classes de trafic (Diffserv)

Flow Label (20 bits) : permet à la source d'identifier une suite de paquets qui doivent être traités comme un même flux par le réseau

Payload Length (16 bits) : longueur en octets du paquet après l'en-tête

Next Header (8 bits) : identifie le type d'en-tête qui suit immédiatement l'en-tête IPv6. Il utilise les mêmes valeurs que le champ *Protocol* de l'en-tête IPv4.

Hop Limit (8 bits) : même logique que TTL (en IPv4).

Hop Limit (v6) / TTL (v4)

Lors du forwarding, le paquet doit être jeté si la valeur du Hop Limit/TTL est égale à zéro ou si elle est décrémentée jusqu'au zéro.

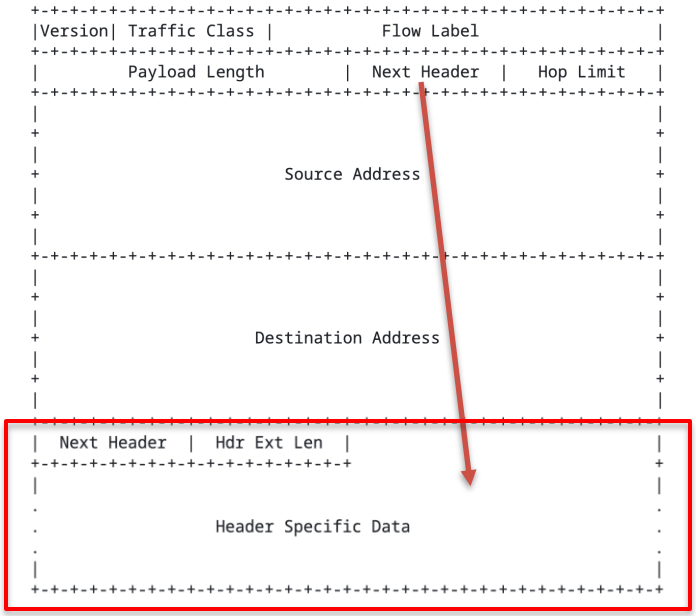
Si Hop Limit/TTL atteint 0 :

- Le routeur supprime le paquet.
- Un message ICMP « Time Exceeded » est renvoyé à la source (traceroute).

Le TTL est décrémenté :

- Par chaque routeur sur le chemin vers la destination.
- Le destinataire final ne décrémente pas le TTL, il traite le paquet normalement, même si le TTL est 0.

En-têtes optionnelles IPv6 (*RFC 6564*)



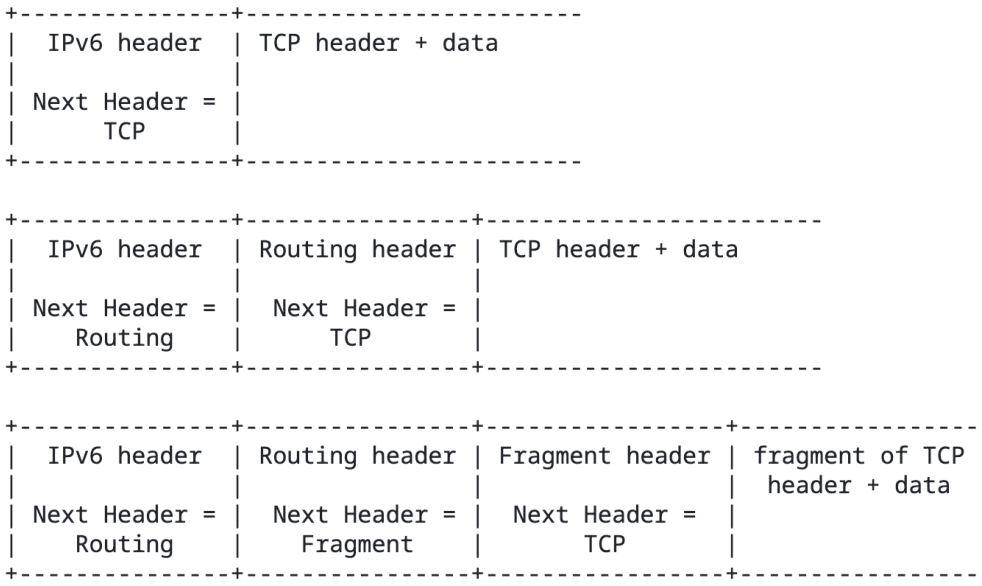
Plusieurs Next Headers possible

Next Header (8 bits) : identifie le type d'en-tête qui suit

Hdr Ext Len (8 bits) : length of the extension header, exprimée en unité de 8 octets, sans compter les 8 premiers octets

Header Specific Data : peut avoir une longueur variable

En-têtes optionnelles IPv6



Next Header	Protocol/ Extension
6	TCP
17	UDP
58	ICMPv6
43	Routing
44	Fragment

IPv6 auto-configuration

Deux possibilités :

- SLAAC (Stateless Address Auto-Configuration)
  RFC 4862
  Le terminal construit son adresse IP à partir de l'adresse MAC et le préfixe réseau diffusé par le routeur local. (EUI-64)

- DHCPv6 (Stateful)
  RFC 8415
  Contrôle strict de l'attribution des adresses

Mécanisme EUI-64

EUI-64 est un mécanisme permettant de générer l'adresse IPv6 à partir de :

- Préfixe annoncé par le routeur
- Adresse MAC de l'hôte

On insère *FF:FE* au milieu de l'adresse MAC puis on *inverse le bit U/L* du premier octet.

Exemple :
L'adresse MAC : 00:11:22:33:44:55, le préfixe annoncé : 2001:DB8:ABCD:1::/64
On insère FF:FE au milieu de l'adresse MAC -> 00:11:22:FF:FE:33:44:55
Puis, on inverse le bit U/L 02:11:22:FF:FE:33:44:55
L'adresse générée : 2001:DB8:ABCD:1:0211:22FF:FE33:4455/64

UVSQ

université PARIS-SACLAY

NDP
(Neighbor Discovery Protocol)

NDP

NDP (Neighbor Discovery Protocol)
RFC 4861

NDP remplace ARP, ICMP Router Discovery et Router Redirect de IPv4.
Fonctionnalités :

- Localiser les équipements de routage
- Découverte de préfixes
- Autoconfiguration d'adresses
- Détection de duplication d'adresse (DAD)
- …

Message NDP

- Router Solicitation
  Un hôte demande aux routeurs du lien d'envoyer une Router Advertisement.
  Multicast : tous les routeurs dans le réseau (FF02::2)

- Router Advertisement
  Un message envoyé par le routeur pour annoncer des informations essentielles sur le réseau (passerelle par défaut, préfixe, MTU …)
  Multicast : tous les nœuds dans le réseau (FF02::1)
  Le routeur envoie des Router Advertisements périodiquement, ou en réponse à un message Router Solicitation.

Message NDP

- Neighbor Solicitation
  Un message utilisé pour :
  1) découvrir l'adresse MAC d'un voisin (remplace ARP)
  2) vérifier qu'une adresse IPv6 n'est pas déjà utilisée (DAD)
  3) détecter la joignabilité d'un voisin (NUD : Neighbor Unreachability Detection)

- Neighbor Advertisement
  La réponse au Neighbor Solicitation.
  Neighbor Advertisement fournit l'adresse MAC en réponse à un Neighbor Solicitation, mais il sert également à confirmer la joignabilité d'un voisin dans le cadre de NUD.

Résumé (Cours 8)

- NAT
- IPv6
- NDP