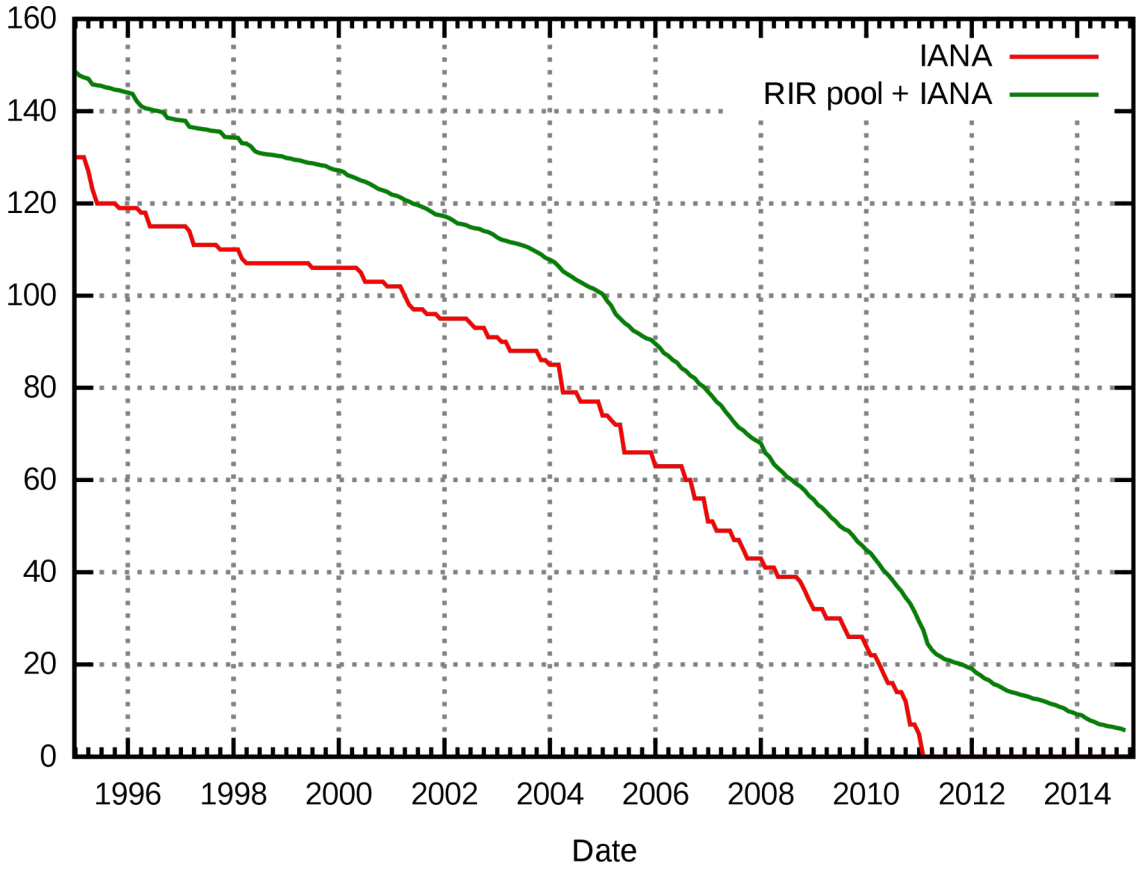
Introduction à IPv6

Jean-Patrick Gelas - Université de Lyon

Sources

- Livres :
  - Réseaux (3ème édition), Andrew Tanenbaum, Dunod.
  - Réseaux & Télécoms, Claude Servin, 2ème édition, Dunod.
  - IPv6, théorie et pratique, O'Reilly.
- Documents :
  - https://fr.m.wikipedia.org/wiki/IPv6
- Vidéos :
  - FormIP : Types d'adresses et préfixe IPv6
    https://www.youtube.com/watch?v=ATOk49wBKJM
  - FormIP : IPv6 utilise les protocoles NDP, ICMPv6 et le Multicast pour découvrir le réseau
    https://www.youtube.com/watch?v=Sb_zoFp725o

Motivations



- Depuis 2011 → Grosse pénurie ! Les 5 derniers blocs d'adresses ont été alloués en février 2011 par l'IANA
- IPv6 est disponible depuis le début des années 90...
- En 2000 le transfert aurait pu être fait (mais à l'époque encore beaucoup d'adresses disponibles)...

Introduction

- Pour éviter la pénurie on utilise le NAT/PAT depuis des années.
- CIDR a également permit de repousser l'échéance de quelques années.

- Mais Internet utilisé par un nombre toujours plus grand d'individus et de systèmes exprimant des besoins différents.
- Convergence de l'ordinateur, des réseaux, des capteurs, de l'audiovisuel et de l'industrie des loisirs.
- Le protocole IP doit évoluer et devenir plus flexible.

Introduction

En 1990, l'IETF débute les travaux d'une nouvelle version du protocole IP

- qui ne devrait jamais être en rupture d'adresses,
- qui devrait résoudre toute une variété de problèmes nouveaux et
- offrir plus de flexibilité et d'efficacité.

Objectifs de ce nouveau protocole
(1/2)

- Supporter des milliards d'ordinateurs en se libérant de l'inefficacité de l'espace des adresses IP actuelles.
- Réduire la taille des tables de routage.
- Simplifier le protocole pour permettre aux routeurs de router les datagrammes plus rapidement.
- Fournir une meilleur sécurité (authentification et confidentialité).
- Accorder plus d'attention au champ *Type de Service* (ex: trafic temps réel)

Objectifs de ce nouveau protocole
(2/2)

- Faciliter la diffusion multi-destinataire (*multicast*).
- Sécuriser les communications.
- Donner la possibilité à un ordinateur de se déplacer sans changer son adresse (mobility).
- Permettre au protocole une évolution future.
- Accorder à l'ancien et au nouveau protocole une coexistence pacifique.

IPv6 répond à la majorité des objectifs

- En 1993, **IPv6** ou **IPng** (*next generation*) proposé par *Deering* et *Francis* (SIPP *Simple Internet Protocol Plus*) répondait raisonnablement aux objectifs édictés.
- IPv6 n'est généralement pas compatible avec IPv4 mais compatible avec tous les autres protocoles Internet (TCP, UDP, ICMP, IGMP, OSPF, BGP et DNS).
- Parfois de légères modifications sont requises (pour fonctionner avec de longues adresses).

Principales caractéristiques d'IPv6

- Des adresses plus longues : 128 bits contre 32 bits pour IPv4.
- Simplification de l'en-tête des datagrammes (7 champs contre 13). Permet au routeur de traiter les datagrammes plus rapidement et améliore globalement leur débit.
- Plus de souplesse aux options. Des champs obligatoires d'IPv4 deviennent optionnels. Les options sont représentées différemment (ce qui permet aux routeurs d'ignorer plus simplement les options qui ne leur sont pas destinées).
- La sécurité : Authentification et confidentialité.
- Une grande attention à été porté aux Types de Services.
- *Broadcast* d'IPv4 abandonné au profit du *Multicast*.

Structure d’une adresse IPv6

- Une adresse IPv6 au format binaire :
  128 bits découpés en 8 groupes de 16 bits.

```
0010000111011010 0000000011010011 0000000000000000
0000000000000000 0000001010101010 0000000011111111
0000000000000000 1001110001011010
```

Structure d’une adresse IPv6

- Chaque groupe de 16 bits est converti en nombre hexadécimal et séparé par des caractères ':'.

```
0010000111011010 0000000011010011 0000000000000000
0000000000000000 0000001010101010 0000000011111111
0000000000000000 1001110001011010
```

21DA : 00D3 : 0000 : 0000 : 02AA : 00FF : 0000 : 9C5A

Structure d’une adresse IPv6

- Les zéros à gauche de chaque groupe peuvent être supprimés. Cependant chaque bloc doit avoir au moins un chiffre individuel.

```
0010000111011010 0000000011010011 0000000000000000
0000000000000000 0000001010101010 0000000011111111
0000000000000000 1001110001011010
```

21DA : 00D3 : 0000 : 0000 : 02AA : 00FF : 0000 : 9C5A

21DA:D3:0:0:2AA:FF:0:9C5A

Structure d’une adresse IPv6

- Une séquence contiguë de 0 peut être remplacé par '**::**' une unique fois.

```
0010000111011010 0000000011010011 0000000000000000
0000000000000000 0000001010101010 0000000011111111
0000000000000000 1001110001011010
```

```
21DA : 00D3 : 0000 : 0000 : 02AA : 00FF : 0000 : 9C5A
```

21DA:D3:0:0:2AA:FF:0:9C5A

21DA:D3::2AA:FF:0:9C5A

Structure d’une adresse IPv6

- ID réseau
  - **Préfixe** de site
  - Préfixe de sous réseau (inclut les bits de sous réseau défini par l’administrateur)
- ID hôte
  - Configuré manuellement ou
  - Automatiquement (aléatoire ou EUI64)
- Notation CIDR
- Masque (ex: /64)

Types d’adresses

- **Unicast** : Une adresse unicast désigne une interface pour des communications point-à-point classique. Elle peut être utilisée pour identifier un groupe d'interfaces lorsque ces interfaces constituent une agregation de liens.
- **Multicast** : Diffusion d’un hôte vers **une sélection** d’hôtes.
- **Anycast** : Un hôte communique avec **un** hôte du groupe le plus proche (au sens du routage). C’est une adresse virtuelle qui pointe sur une ou plusieurs adresses physique.

Remarque : Une interface peut avoir plusieurs adresses de types différents.

Types d'adresses : Unicast

- *Link Local Address* (LLA) : **FE80 : : …**
  Un hôte a au minimum une adresse de ***lien local*** qui permet de :
  - communiquer avec les voisins de son domaine de diffusion,
  - découvrir son routeur de voisinage

    Attention : Ces adresses ne sont pas routable !
  - Il peut exister plusieurs adresses link-local sur des liaisons différentes d'une même machine. On lève les ambiguïtés en fournissant un indice de zone. *Exemple* : FE80 : : 3%**eth0**
- *Unique Local Address* (ULA) : **FD00 : : …**
  - Une adresse **locale unique** est routable sur site. Mais ne peut pas traverser le routeur de bordure.
  - Correspond aux adresse privées de IPv4 (RFC1918)
  - Elles peuvent être définie :
    - En « dur »
    - DHCPv6
    - Auto configurée via le préfixe transmis par le routeur.

Types d'adresses : Unicast (suite)

- *Global Unicast Address* (GUA) :
  Une **adresse globale** routable sur Internet !
  IANA → 2000: :/3
  RIR → /12 à /23
  LIR (FAI) → /48
  affecté à un hôte local → /64

  ~~NAT / PAT~~ inutiles !
  A nouveau une connexion de bout en bout !

- *Loopback address* (adresse de bouclage) : **: : 1** ou 0:0:0:0:0:0:0:1 équivalent de 127.0.0.1 en IPv4.
- *Undefined address* (adresse non spécifiée) : **: : /128** ou 0:0:0:0:0:0:0:0, correspond à l'adresse 0.0.0.0 d'IPv4 qui désigne une interface en cours d'initialisation.
- **2001:db8::/32** utilisé spécifiquement dans les exemples de documentation.

Types d'adresses : Multicast

- Ou adresse de *Multidiffusion* en français. La notion de *broadcast* disparait car trés pénalisante en terme de performance réseau.
- 12 bits **FF0** en préfixe
- 4 bits qui définissent l'étendu (*cf.* exemples ci-dessous)
- 112 bits pour identifier le groupe

Exemples :
0
1
2 (node-local) FF0**2 : :**1:2 → Serveur DHCP du site.
…
…

E (global) FF0**E : :** 101 → tous les serveur NTP de l'internet
…
F

Scope : Domaine de validité et d'unicité

- Adresses **unicast** :
  - Loopback (::1) a une validité limitée à l'hôte.
  - Link-local (FE80::) : uniques sur un lien donné.
  - Les adresses **locales uniques** (FD00::) on un scope **site**.
  - Les autres adresses ont un scope **global**
- Adresses **anycast** : idem adresses *unicast*
- Adresses **multicast** (FF0::/12) : les bits 13 à 16 déterminent le scope (local, lien, organisation ou global).

En pratique : ifconfig

- At home (free)

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
         ...


wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.22  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::c3b1:b33d:749a:4fc4  prefixlen 64  scopeid 0x20<link>
        inet6 2a01:e0a:588:2660:34f3:13c9:dce:764d  prefixlen 64 scopeid 0x0<global>
        ether 9c:b6:d0:8d:e9:c9  txqueuelen 1000  (Ethernet)
         ...
```

- Renater : Préfixe 2001:660::/32 (RIPE NCC)

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 34:15:9e:36:dd:24
    inet6 fe80::3615:9eff:fe36:dd24%en0 prefixlen 64 scopeid 0x4
    inet6 2001:660:5001:142:3615:9eff:fe36:dd24 prefixlen 64 autoconf
    inet 134.214.143.142 netmask 0xfffffe00 broadcast 134.214.143.255
    media: autoselect (100baseTX <full-duplex>)
    status: active
```

Mécanismes de Découverte du réseau

- En IPv6 plus de pouvoir donné aux équipement réseau.

IPv4	IPv6
ARP + broadcast	NDP (Neighbour Discovery Protocol), ICMPv6 et Multicast

Mécanismes de Découverte du réseau : NDP

- NDP (Neighbour Discovery Protocol) : 4 fonctions

  1. Router solicitation (multicast) + Router Advertisment

  2. Neighbour Solicitation + Neighbour Advertisment (équivalent ARP)

  3. DAD (Duplicate Address Detection)

  4. SLAAC (Stateless Address Auto config), permet de découvrir l'adresse IPv6 que l'hôte devra utiliser + sa passerelle. ATTENTION : Manque le DNS !

Mécanismes de Découverte du réseau : DHCPv6

- Un serveur DHCPv6 peut fonctionner en deux modes
  - **Stateless** pour fournir seulement les adresses des serveurs DNS
  - **Stateful** dont le fonctionnement est similaire au DHCP classique
- Messages DHCP (Stateful)

DHCP v4		**DHCP v6**
Discover	→	**Solicit** : l'hôte utilise ce msg pour découvrir le srv DHCPv6
Offer		**Advertise** : donne à l'hôte une @IPv6, une dflt gw, DNS
Request		**Request** : permet à l'hôte de demander si il est autoriser à utiliser ces infos.
Ack		**Reply** : message de réponse du serveur pour donner sa confirmation.

Durée de vie

- Les adresses IPv6 associées à une interface ont une durée de vie déterminée (en général infinie).
- Une durée de vie (*préférée* et de *validité*) peut être configurée dans les routeurs qui fournissent des préfixes pour la configuration automatique.

  Ex: En combinaison avec un changement DNS, permet une transition progressive vers une nouvelle adresse IPv6 sans interruption de service.

  Préférée → n'est plus utilisé pour les nouvelles connexions.
  Validitée → supprimée de la configuration de l'interface.

Neighbour Discovery Protocol

- Associe les adresses IPv6 à des adresses MAC sur un segment (comme ARP pour IPv4).
- Permet de découvrir les routeurs et les **préfixes routés**, le MTU, les adresses dupliquées, les hôtes devenus inaccessibles, **l'autoconfiguration des adresses**, les serveurs DNS.
- Il s'appuie sur ICMPv6.

Nodes Network configuration scenario

- IPv6 (Scope: Link) address is used to discover its neighbourhood (broadcast domain). Two methods:
  - **Router advertisment** : node obtains from the router an address (with a given prefix) and a route to access the network.
  - **DHCPv6** : works like IPv4 DHCP. The server DHCP assigns an address and a route in function of the node network identification. This allows to keep a trace of network assignations.

Network interface is now fully configured with an IPv6 link address and IPv6 **Site** address.

Network interface auto-configuration

- Router advertisement daemon: **radvd**.
- One daemon per LAN must be installed.
- The daemon advertise its presence through regular announcements. Clients received them and configure themselves with the received prefix.
- A simple *radvd.conf* file:

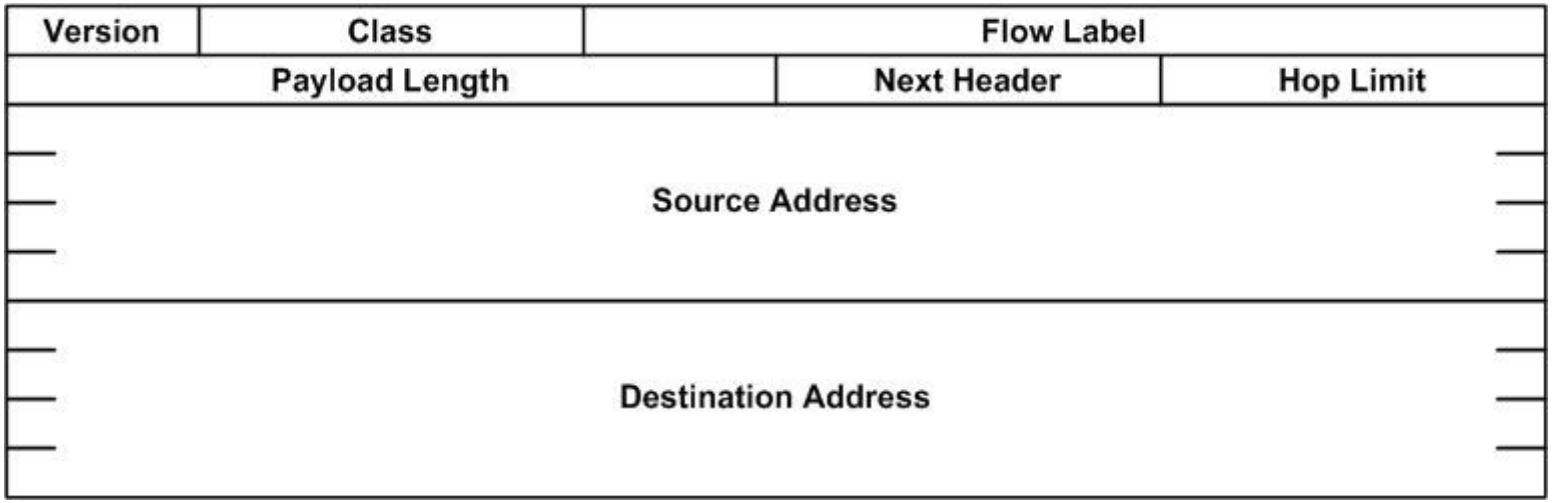
```
interface eth1 {
   AdvSendAdvert on;
   prefix fd0e:ebc6:bc71:0401::/64 {};
};
```

Le datagramme IPv6
Simplification des traitements par le routeur

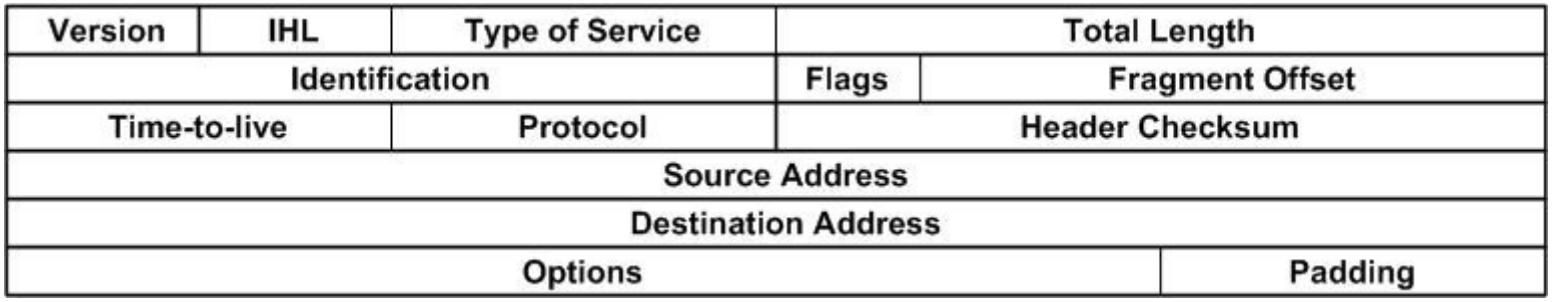
- Pour améliorer le traitement des datagrammes dans les routeurs :
  - L'en-tête a une longueur constante (40 octets).
  - Suppression du champ option et des champs devenus inutiles (ex: le champ IHL d'IPv4)
- La somme de contrôle a été supprimée.
  - En IPv4 la somme de contrôle inclut le champ TTL ce qui implique son recalcul dans chaque routeur.
  - Le mécanisme de contrôle de TCP incluant un pseudo en-tête IP est suffisant pour protéger les adresses.
- Le champs TTL est renommé en *Hop Limit*.

En-tête IPv6 et IPv4

IPv6



IPv4



Structure du datagramme IPv6

- Le champ TOS *(Type of Service)* trouve son équivalent en deux champs :
  - classe de trafic, **CoT** *(Class of Traffic)* sur 8 bits et un
  - identifiant du flux *(Flow Label)* attribué par la source (notion de circuit virtuel de type *soft-state*).
- Le champ *Protocol* est remplacé par l'indication du type de l'en-tête suivant *(Next Header).*
  - Si aucune option n'est invoquée, il contient l'identification du protocole transporté (Ex: TCP, UDP, IPv4, ICMP).
- Un compteur de saut (*Hop limit*) positionné par la source (à 64) et décrémenté de 1 par chaque noeud intermédiaire (remplace le champ TTL). Le paquet est détruit si égale à 0.

Le datagramme IPv6
La fragmentation

- Les données relatives à la fragmentation (ID, flags, offset) disparaissent.
- IPv6 implémente un mécanisme de découverte de la MTU (si le paquet est trop gros, l'émetteur reçoit un paquet ICMPv6 *Packet Too Big*).
- Si nécessaire, la fragmentation est réalisée par la source et le réassemblage par le destinataire ce qui allège le travail des routeurs intermédiaires.
- Si la fragmentation par le réseau s'avère indispensable, une extension de l'en-tête est prévue.

Le datagramme IPv6
Traitement des options ou en-têtes d'extension

- Des extensions d'en-tête remplacent les options d'IPv4.
- **Ces options sont ignorées des routeurs** sauf l'extension *Hop-by-hop* (proche en proche) qui est traitée par tous les routeurs.
- Les extensions doivent apparaître dans un ordre prédéfini (Hop-by-hop doit apparaître en premier).

Valeur	Type	Désignation
0	option	Hop-by-hop
4	protocole	Ipv4
6	protocole	TCP
17	protocole	UDP
43	option	Routing header
44	option	Fragment header
45	protocole	Interdomain routing protocol
46	Protocole	RSVP
50	option	IPSec Encapsulation
51	option	IPSec Authentification

Le datagramme IPv6
Exemple d'extension d'en-tête

Extension **Proche en Proche** ou ***Hop-by-Hop*** (0)

- Cette extension est la seule à être traitée par tous les routeurs traversés.
- La longueur de l'extension *(Length)* est exprimé en mots de 64 bits – 1 mot.
- Cette extension est un champ d'options au format TLV.
- Les différentes options sont :
  - Des champs de bourrage, type 0 pour 1 octet de bourrage, type 1 pour une longueur de plus de 2 octets (alignement de l'extension sur un multiple de 64 bits)
  - ***Router Alert*** (type 5), utilisée pour indiquer au routeur qu'il doit examiner le contenu du champ données (message ICMP ou RSVP).
  - ***Jumbogramme*** (type 194), ce champ d'extension spécifie la longueur des données (sur 4 octets) quand celle-ci dépasse 64ko (dans ce cas le champ Payload Length est mis à 0).

Le datagramme IPv6
Exemple d'extension d'en-tête

Extension **Routage** (43)

- Cette extension permet d'imposer une route à un paquet.
- Actuellement seul le routage par la source est défini (type 0).
- L'extension routage par la source contient une liste de routeurs à traverser.
- Ce routage peut-être soit strict (le routeur voisin doit être le suivant), soit lâche *(loose),* le routeur peut alors consulter ses tables pour choisir la route à prendre pour joindre le routeur suivant.
- Utilisé par Mobile IPv6.

Le datagramme IPv6
Exemple d'extension d'en-tête

Extension **Destination** (60)

- Cette extension est traitée par le destinataire.
- Elle introduit le concept de mobilité du destinataire, un mobile pouvant toujours être joint par son adresse principale.
- Les options destinations permettent de gérer l'association entre une adresse locale sur le réseau d'accueil et l'adresse principale du mobile.

Attribution des adresses IPv6

dans un sous réseau

- Configuration manuelle : L'administrateur fixe l'adresse.
- Configuration automatique :
  - Autoconfiguration sans état basé sur l'adresse MAC (suscite des inquiétudes)
  - Autoconfiguration avec tirage pseudo-aléatoire (adresses temporaire modifiées régulièrement).
  - Adresse généré cryptographiquement (clé publique).
  - Attribution par un serveur DHCPv6.

Multicast

- Rappel : Le multicast permet de diffuser un paquet à un groupe. Il évite l'usage intempestif de *broadcast* qui pénalise les performances.
- Remarque : Il n'y a plus d'adresse *broadcast* en IPv6.
- Exemple : FF02::101 permet de contacter les serveurs NTP sur un lien.
- Ethernet : Une série de préfixe OUI est réservé aux adresses IPv6 (33:33:xx).
- Le routage au-delà du segment requiert l'utilisation de protocoles de routage comme PIM.

DNS

- Les noms d'hôtes sont associés à des adresses IPv6 grâce à l'enregistrement AAAA.

```
www.ipv6.ripe.net.      IN AAAA   2001:610:240:22::C100:68B
```

- Enregistrement inverse (adresse inversé sous forme canonique).

```
b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa.  IN PTR www.ipv6.ripe.net.
```

  La résolution inverse peut être utilisée par des systèmes de **contrôle d'accès** ainsi que par des **outils de diagnostic** comme *traceroute*.

- Bind9 prend en charge les records AAAA ainsi que le transport des requêtes sur IPv6.

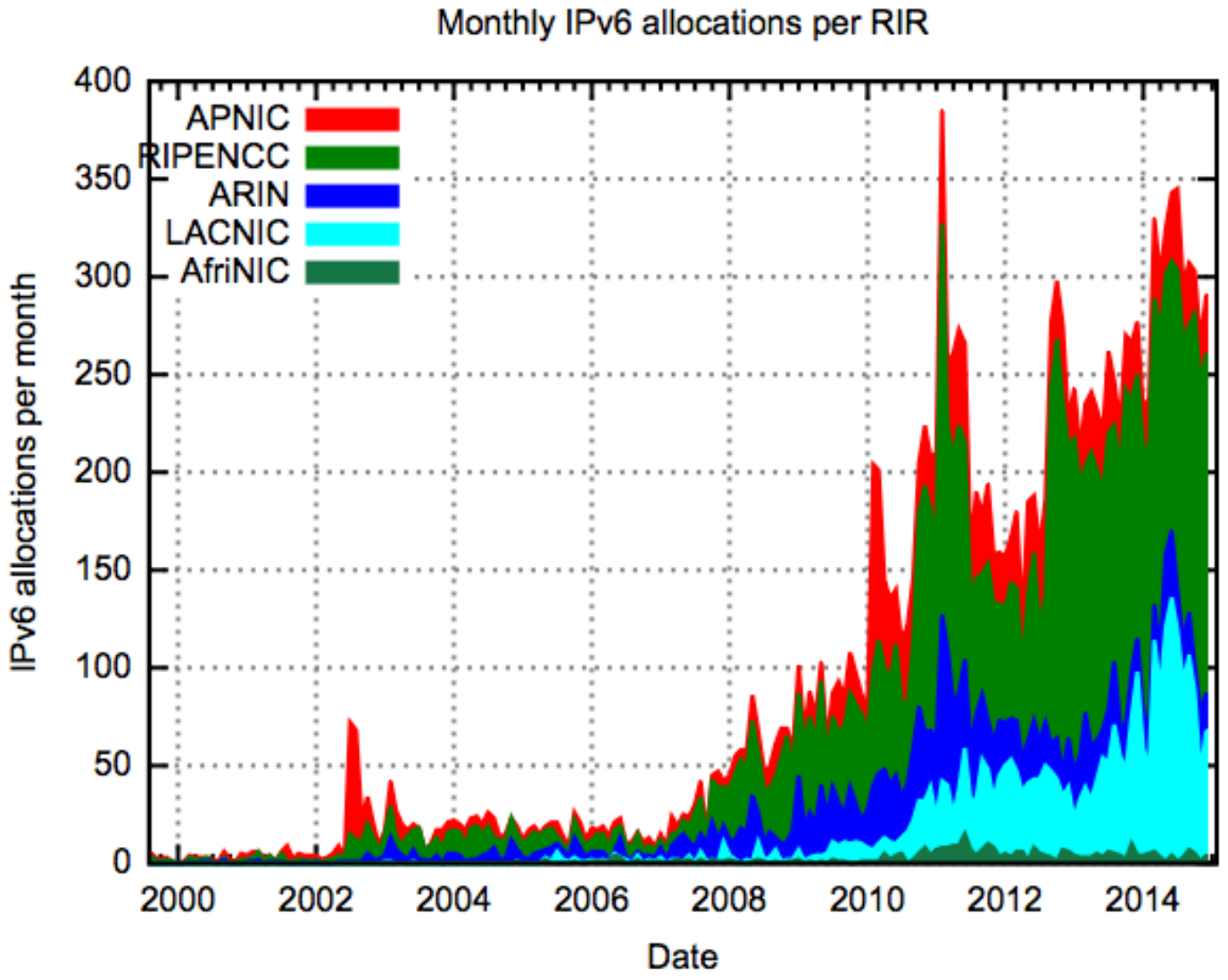
Protocoles de routage

- Les protocoles de routage ont été mis à jour pour IPv6.
  - BGP,
  - OSPFv3,
  - IS-IS,
  - MPLS

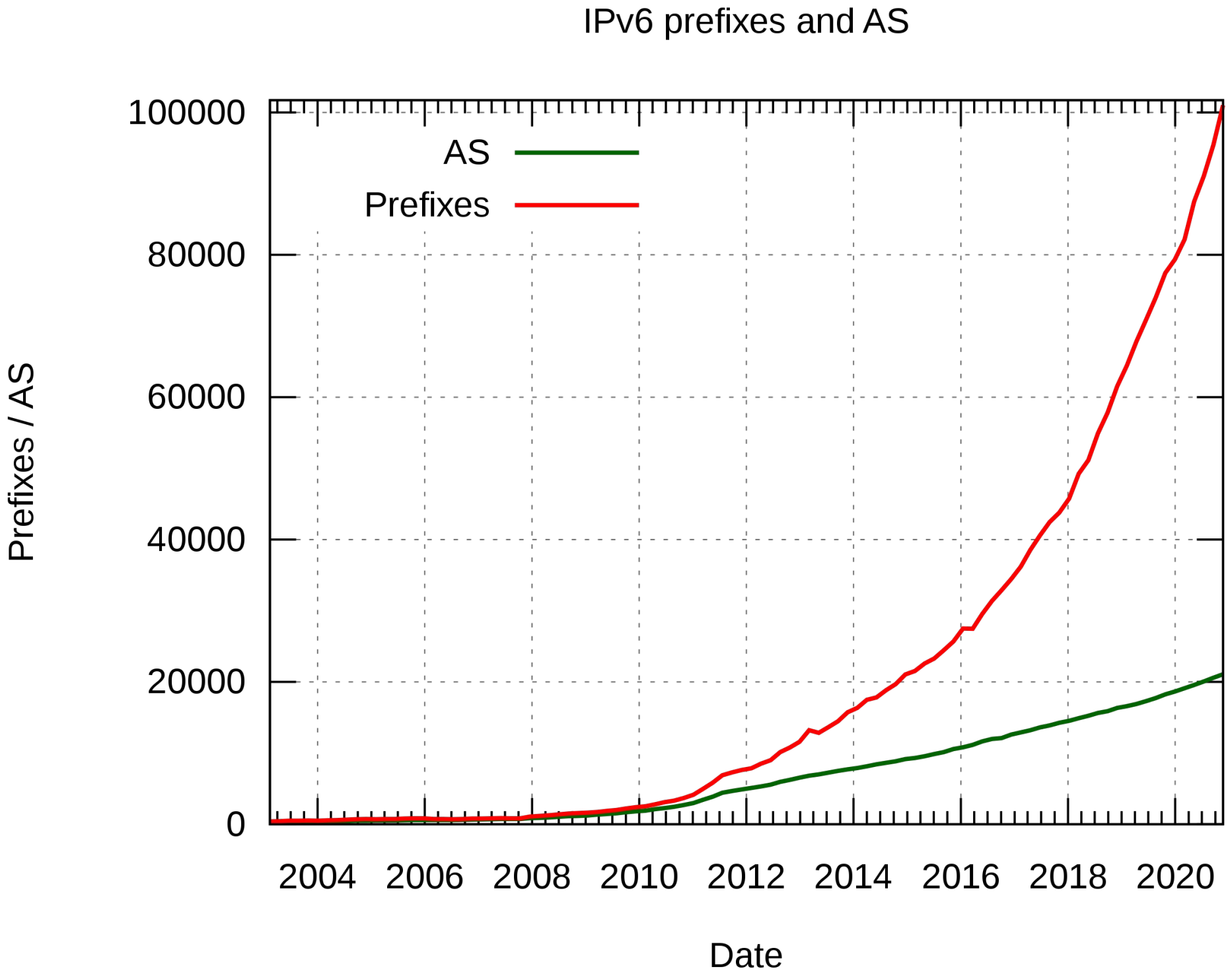
Couches Transport et Liaison

- TCP et UDP fonctionnent comme en IPv4.
- Le pseudo en-tête utilisé pour le calcul du code de contrôle est cependant modifié et inclut les adresses IPv6 source et destination.
- L'usage du code de contrôle est obligatoire même pour UDP.
- Des modifications mineurs ont été apportées pour la prise en charge des paquets *jumbo* (> 64ko → 4Go).
- Les protocoles de la couche de liaison de type IEEE 802 sont adaptés pour le transport d'IPv6. Ex: Ethernet, *type* = 0x86DD.
- Les commutateurs ethernet ne nécessitent pas de mise à jour (sauf pour le contrôle et la gestion à distance).

Monthly IPv6 allocations per RIR



- RIPE NCC (Réseaux IP Européens – Network Coordination Center), APNIC (Asia Pacific Network Information Center), ARIN (American registry for Internet Numbers), LACNIC (Latin American and Caribbean Internet Addresses Registry)


IPv6 prefixes and AS
AS
Prefixes
Prefixes / AS
100000
80000
60000
40000
20000
0
2004
2006
2008
2010
2012
2014
2016
2018
2020
Date

Conclusion

- IPv6 est inévitable !
- Répond bien au problème de pénurie d’adresses d’IPv4.
- Améliore la rapidité des communications en simplifiant l’en-tête, la structure des paquets, et l’agrégation de préfixe.
- Meilleurs gestion de la sécurité (IPsec) et de la QoS (marquage des flux).
- Amélioration des aspects de diffusion (multicast)
- Meilleur support des extensions (et options).
- Favorise l'émergence de nouvelles applications (Web of Things (WoT), communications temps réels, ...).

Remarques de fin...

- IPv4 et IPv6 sont incompatibles mais **co-existe (dual stack)**.
- L'utilisation de NAT/PAT n’est plus nécessaire
- Les hôtes peuvent avoir une adresse publique
- Désactivé IPv6 n'accélère pas le fonctionnement d'une machine (activé par défaut).
- IPv6 est prévu pour les machines, quoi que... :)

FE80:FEED:BABE:CAFE:F00D:DEAD:BEEF:42/48

Pour tester...

- http://www.kame.net/ (la tortue devrait nager !)
  - www.kame.net (2001:200:dff:fff1:216:3eff:feb1:44d7),
  - Dans un navigateur : http://**[**2001:200:dff:fff1:216:3eff:feb1:44d7**]**/
- http://www.myipv6.org/
- http://test-ipv6.com/
- http://ipv6.google.com/

Outils et applications pour tester IPv6

- ifconfig (ou ip), ping6, traceroute6, tracepath, tcpdump, route (–inet6 ou –A inet6),...
  - ping6 fec0::2
  - ifconfig eth0 inet6 **add** 2001::1/64
  - ping6 –I eth0 fe80::240:48ff:feb1:c66
  - tcpdump –i eth0 ip6
- iperf, Ethereal/Wireshark, SSH, client/serveur tftp, http,...
  - iperf –s –V
  - iperf –c fec0::1 –V