www.cnrs.fr

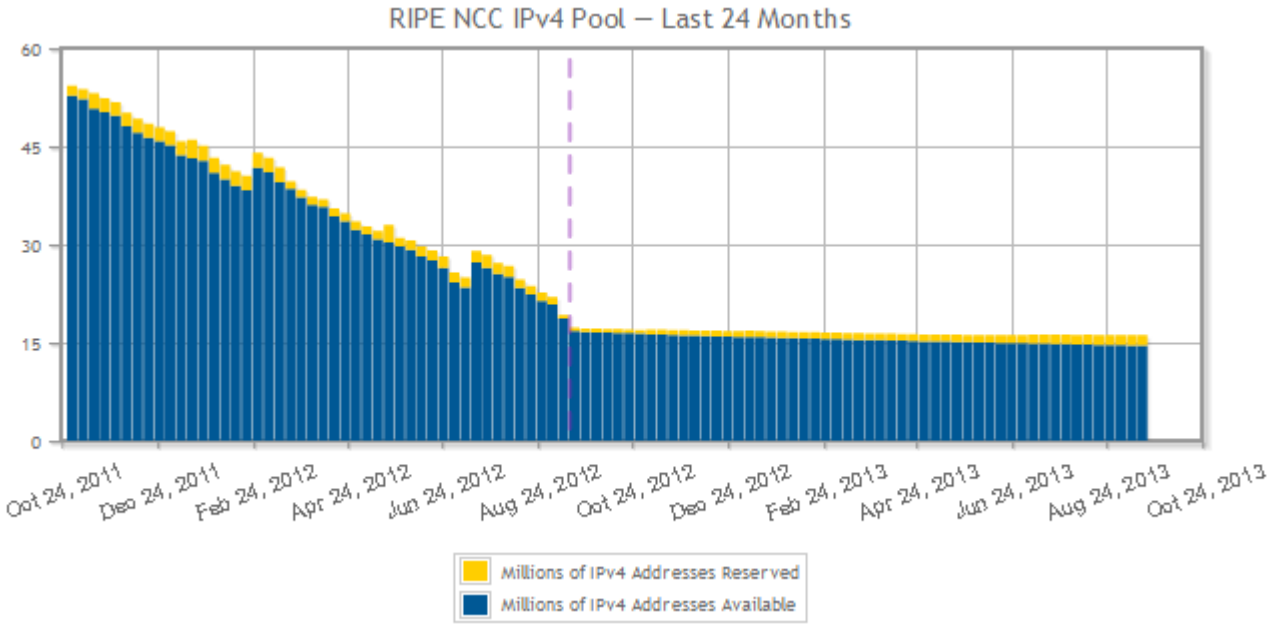
IPv6

Gaël BEAUQUIN

19 septembre 2013

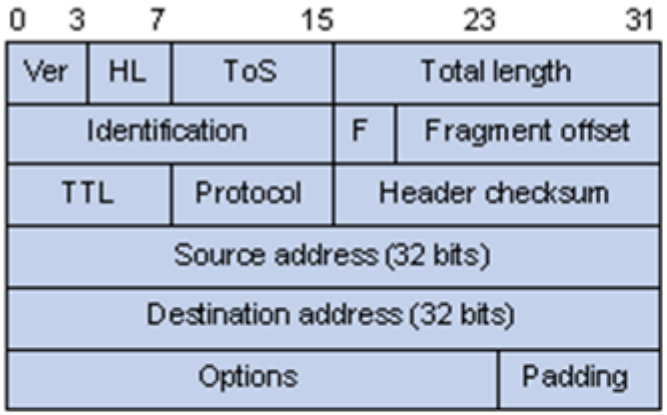
Pourquoi passer à IPv6 ?

- Depuis des années on évoque le spectre de l'épuisement d'adresses IPv4
- Le 3 février 2011, l'IANA attribue un ultime /8 au RIPE NCC
- Le 14 septembre 2012, le RIPE NCC a épuisé toutes les autres adresses, et attaque le dernier /8
- Chaque LIR peut seulement prétendre à un /22 sur ce bloc

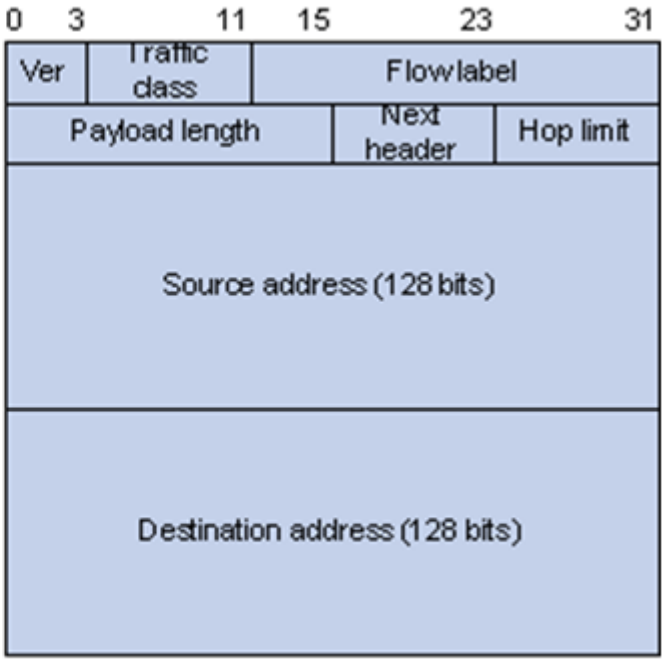


IPv6 en quelques mots

- Fondamentalement similaire à IPv4
- Nouvel en-tête
- Adressage étendu sur 128 bits
- NDP remplace ARP
- Autoconfiguration sans état
- Fonctionnalités intégrées : IPSec, Mobilité



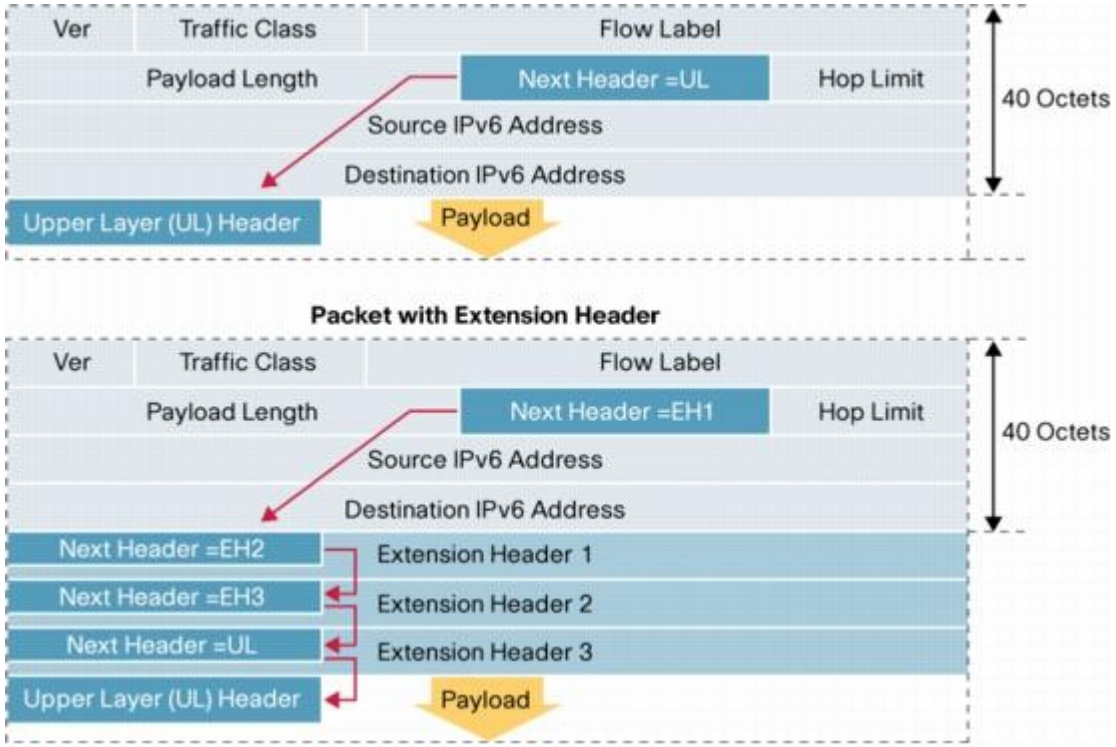
IPv4 header



Basic IPv6 header

Les options IPv6

- Définis par la RFC 2460
- Les options sont chaînées (chaque option indique sa taille et le type de la prochaine option, et en fin de chaîne on indique le protocole de niveau supérieur)
- Par défaut, un routeur intermédiaire ne regarde pas les options
- « Hop-by-Hop Option » indique des options qui doivent être regardée par tous les intermédiaires, « Destination Option » indique des options pour la destination finale


Ver
Traffic Class
Flow Label
Payload Length
Next Header =UL
Hop Limit
Source IPv6 Address
Destination IPv6 Address
Upper Layer (UL) Header
Payload
40 Octets
Packet with Extension Header
Ver
Traffic Class
Flow Label
Payload Length
Next Header =EH1
Hop Limit
Source IPv6 Address
Destination IPv6 Address
Next Header =EH2
Extension Header 1
Next Header =EH3
Extension Header 2
Next Header =UL
Extension Header 3
Upper Layer (UL) Header
Payload
40 Octets

Les autres options

- Routing Header : permet de faire du source routing, et utilisé pour la mobilité IPv6
- Fragment Header : gestion des paquets fragmentés
- Authentication Header et Encapsulating Security Payload Header : utilisés pour les fonctions IPSec
- Mobility Header : utilisé pour la mobilité IPv6

Adressage étendu sur 128 bits

- Réseaux étouffés par NAT/PAT
- Des adresses à ne plus savoir qu'en faire !
- Adresse 2001:0db8:0000:85a3:0000:0000:ac1f:8001 qui peut être réduite en 2001:db8:0:85a3::ac1f:8001
- Utilisation de [ ] pour éviter d'éventuelles confusions : http://[2001:db8:0:85a3::ac1f:8001]/
- Une machine peut obtenir toute seule une adresse publique
- Plus de broadcast, mais de nouveaux multicasts et le concept d'anycast
- Notion d'adresses « global » et « link-local » (notion « site-local » est obsolète)

Multicasts

- Définis par la RFC 4291
- Une adresse multicast commence par FF, et est suivi d'un code qui indique la portée (FF01 indique un multicast node-local, FF02 indique link-local, etc)
- FF02::1 adresse tous les hôtes sur le même réseau, utilisé par exemple pour les Router Advertisement
- De multiples adresses sont définies pour le routage (all-routers, rip-routers, pim-routers, etc) ou trouver les adresses MAC des autres machines
- Mais aussi pour des protocoles comme DHCP ou NTP (FF02::101 adresse tous les serveurs NTP sur le réseau)
- Liste exhaustive : http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

NDP et ICMPv6

- NDP est défini par la RFC 4861 et ICMPv6 par la RFC 4443
- NDP remplace ARP, et fait partie de ICMPv6
- Utilisation d'un multicast « solicited-node » pour trouver l'adresse MAC, au lieu du broadcast d'ARP
- ICMPv6 reprend ARP et ICMP, mais également IGMP
- Version sécurisée de NDP, SEND avec des CGA (Cryptographically Generated Addresses), définie par la RFC 3971, peu déployée

Autoconfiguration sans état

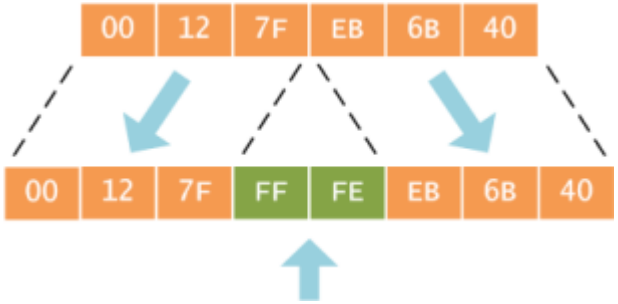
- Un poste IPv6 peut se trouver une adresse unique tout seul
- Il obtient son adresse et celle du routeur, mais pas de DNS
- Utilisation du DNS obtenu avec l'IPv4
- Extension RDNSS (non implémenté par Cisco/Juniper, rdnssd-win32 disponible pour Windows)
- DHCPv6 statefull (adresse IP + DNS) ou stateless (juste DNS)
- Client DHCPv6 pas forcément pratique à déployer, nécessité de commande en ligne pour Windows, package à installer pour Linux

Autoconfiguration sans état

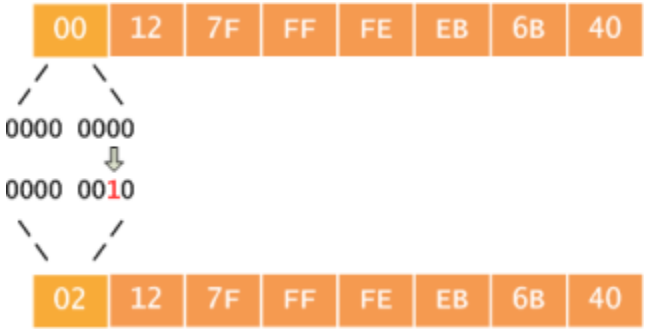
- Génération d'une adresse link-local (fe80::)
- Vérification de l'unicité de l'adresse : envoi d'un message Neighbor Solicitation, réponse Neighbor Advertisement si adresse déjà utilisée
- Solicited-Node address : une adresse multicast de la forme FF02::1:FFxx:xxxx, les 6 derniers digits correspondent aux 6 derniers digits de l'adresse IPv6 correspondante
- Prise de contact avec un Routeur (écoute d'un message Router Advertisement, ou demande d'un paquet RA avec un message Router Solicitation)
- Avec les infos du RA (adresse, préfixe), la machine peut se créer sa propre adresse publique

Création d'un identifiant EUI-64 unique

- On prend l'adresse MAC que l'on coupe en 2, et on ajoute 0xFFFE entre les 2 parties afin de le distinguer d'un EUI-64 « normal »



- Le flag « global » d'une EUI-64 est à 0 pour indiquer une adresse unique. On l'inverse afin que 1 = adresse unique. Ainsi, si on doit créer manuellement un EUI-64, le bit devra être à 0, et on pourra avoir une adresse fe80::1 au lieu de fe80::0200:1



Découverte du PMTU (Path Maximum Transmission Unit)

- Recherche de la plus grande MTU possible pour atteindre une destination
- IPv6 garantit un MTU de 1280 octets
- Envoie de paquets de taille décroissante, jusqu'à ne plus provoquer de réponses ICMPv6 « packet too big »
- Recalcul du PMTU de temps en temps, ou si un changement de route provoque des erreurs.

Protocoles de routage

- La plupart des protocoles de routages ont une version IPv6 : RIPng, ISIS, OSPFv3, EIGRP, BGP…

```
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 no ip address
 speed auto
 ipv6 address 2003::1/124
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/0
 no ip address
 ipv6 address 2002:ABAB::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 2
!
ipv6 router ospf 1
 router-id 1.1.1.1
 area 2 stub no-summary
!
```

```
 router bgp 101
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 1202:ABCD::21B:54FF:FEA9:24B0 remote-as 202

!--- Configures SP-A as neighbor.

 neighbor 1202:ABCD::21B:54FF:FEA9:24B0 ebgp-multihop 2
 neighbor 2303:ABCD::21B:54FF:FE54:FB10 remote-as 303

!--- Configures SP-B as neighbor.

 !
 address-family ipv6
  neighbor 1202:ABCD::21B:54FF:FEA9:24B0 activate
  neighbor 2303:ABCD::21B:54FF:FE54:FB10 activate
  network 1010:1010::/64
  network 2020:2020::/64
 exit-address-family
!
```

Procédure de mise en place

- Inventaire matériel / logiciel, et mise à jour si besoin
- Obtenir un préfixe
- Etablir un plan d'adressage
- Router le préfixe en entrée du réseau
- Mise en place d'ACLv6
- Activer l'IPv6 sur sous-réseau de test
- Déployer l'IPv6 progressivement sur les différents sous-réseaux

Inventaire

- Windows XP et GNU/Linux gèrent IPv6 (souvent activé par défaut)
- Les principaux logiciels serveurs gèrent l'IPv6 (Apache, BIND, MySQL, openLDAP, Postfix…)
- IPv6 > IPv4 si les deux sont disponibles
- IPv6 est souvent « géré » par les équipements réseaux
- Attention au support IPv6 en software (problème de performances en cas de charge) ou au support partiel (fonctionnalités IPv4 pas dispo en IPv6).

Obtenir un préfixe et le faire router

- Renater fournit un préfixe /48 à tous les établissement qui sont connectés sur son réseau
- https://services.renater.fr/connectivite/allocation_d_adresses
- Pour demander le routage sur Renater il faudra passer par SAGA : https://services.renater.fr/connectivite/routage_d_adresses
- A moins d'être connecté directement à Renater, il faudra également faire router le préfixe sur les routeurs intermédiaires

Etablir un plan d'adressage

- Diviser votre préfixe en sous-réseaux /64
- Reprendre vos sous-réseaux IPv4 en sous-réseaux IPv6, pour garder un réseau cohérent
- Pour retrouver facilement vos sous-réseaux, utiliser un digit significatif de l'adresse IPv4, ou l'ID du VLAN

ACL v6

- Important de faire avant de déployer effectivement IPv6
- Si vous avez fait un plan d'adressage cohérent, ce sera un « copier-coller » de vos ACLv4
- Utilisation d'un logiciel pour gérer vos ACLs (type Shorewall)

Déployer progressivement l'IPv6

- Tout d'abord sur un sous-réseau de test (test de la tortue sur kame.net)
- Puis pour les postes serveurs, configurer sur chaque machine une adresse IPv6 statique avec déclaration dans votre DNS de records AAAA et PTR.
- Pour les serveurs, utiliser des noms relatifs aux fonctions au cas où un serveur héberge des services compatibles IPv6 et d'autres non compatibles
- Quand les serveurs sont opérationnels, mise en place pour les réseaux « clients ».

Boîte à outils IPv6

- NDPMon : Permet de suivre le traffic NDP et de faire remonter une alarme en cas d'activité louche
- Ntop : Pour suivre l'évolution du traffic lors de la migration de vos réseaux.
- Netcat6 : Version IPv6 de netcat
- IP6Sic : Version IPv6 de ISIC, qui permet de stress test une interface IPv6
- Nessus (scan de vulnérabilités) / Nmap (scan de ports) supportent l'IPv6 depuis longtemps
- Shorewall6 : Gestion des ACL IPv6

www.cnrs.fr

IPv6

Gaël BEAUQUIN

19 septembre 2013