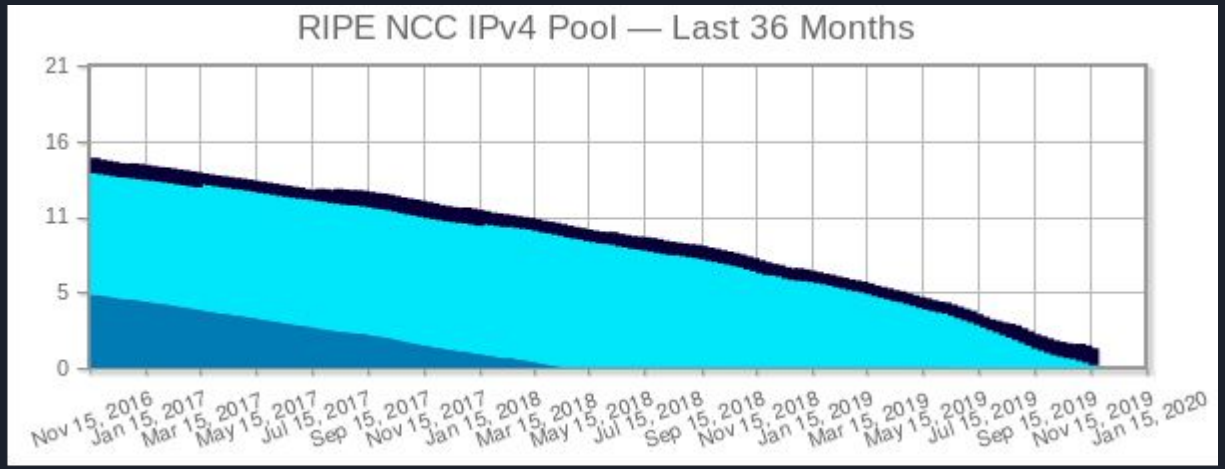
D’IPv4 vers IPv6 : une renaissance

(tardive et complexe…)

Cloud Networking - 3SN-IBDIOT - B. Paillassa [redacted] - Édouard Lumet

IPv4 : où en est on ?

RIPE NCC IPv4 Available Pool	
Millions of IPv4 Addresses in the Pool	1.34
Millions of IPv4 Addresses Available	0.14
Millions of IPv4 Addresses Reserved	1.20



Comment migrer ?

4,3 milliards d'Ipv4 possibles - au moins 3,5 d'allouées.

Comment migrer des équipements à l'échelle opérateur ?

6rd

Qu'est ce ? : **IPv6 Rapid Deployment on IPv4 Infrastructures (RFC 5569)**

Détails : 6to4

Mécanisme de transmission de paquets v6 sur réseaux v4

traduction de l'IPv4 en IPv6 :

Encapsulation du paquet v6 dans le paquet v4

Interconnexion avec réseaux v6 natifs : routeurs spécifiques

annonce du préfixe 2002::/16 avant l'IP traduite

6rd : qu’est-ce ?

Basé sur 6to4, mais reste confiné dans le réseau du FAI qui l’utilise

Objectif : permettre un déploiement d’IPv6 sur le réseau FAI à côté d’IPv4

Mais : pourquoi ne pas juste utiliser 6to4 ? ça existe déjà, et ça doit marcher pas trop mal non ?

ça marche “presque” :

- 6to4 FAI -> internet IPv6 : ok
- 6to4 FAI1 -> 6to4 FAI2 : ok
- Internet IPv6 -> 6to4 FAI : NON

Les améliorations de 6rd

2 axes :

- paquets d'internet v6 entrent uniquement dans les GW 6rd du FAI destination
- tous les paquets v6 à destination d'un client 6rd d'un FAI vont traverser un relai 6rd de ce FAI

Specs :

- Remplacement du préfixe global 2002::/16 par un préfixe appartenant au FAI
- pareil sur les @ip anycast
- routeurs de tête chez les clients supportent IPv6 côté client et 6rd côté FAI

Le fonctionnement

Upgrade les anciens relais et routeurs clients 6to4 en 6rd

Même principe que 6to4 : préfixe IPv6 + adresse IPv4

routage intraFAI : utilise directement l'IPV4

Pour les FAIs qui assignent de l'Ipv4 publique aux clients : pas de pb

Pour les FAIs qui assignent en privé : les paquets ne passent pas par les NATs mais directement relais 6rd

Mais une adresse IPv6, c'est quoi ?

Hexadécimal, 16 octets, 2^128 adresses soit 667M d'IPv6 par millimètre carré

Exemples : 2001:bc8:39b7:100::42, fe80:0000:0000:0000:0ca4:55e8:314f:bc61

Formation des adresses IPv6 en autoconfiguration (stateless) avec EUI-64

Quel(s) inconvénient(s) ? (sécurité)

Exemple réel

Adresse MAC = 00:08:a2:0c:25:4c

Adresse IPv6 autoconfigurée = fe80::208:a2ff:fe0c:254c

Comment palier la perte de confidentialité ? (1)

- Adresse MAC connue globalement
- Pistage et analyse possible (adresse non variable)

Stable and Opaque IIDs with SLAAC (RFC 7217)

- Adresse stable : pour un un même sous-réseau/préfixe d'une même interface
- Adresses différentes : pour chaque préfixe d'une même carte
- Rendre difficile la connaissance d'un IID même sachant un autre IID
- Insensible au changement d'adresse physique
- Concerne uniquement les adresses non temporaires

RID = F(Prefix, Net_Iface, Network_ID, DAD_Counter, secret_key)

Comment palier la perte de confidentialité ? (2)

- *Adresse MAC connue globalement*
- *Pistage et analyse possible (adresse non variable)*

Privacy extensions in SLAAC (RFC 4941)

- Identifiants d'interface aléatoires et temporaires
- Indépendance entre les adresses
- Génération d'un lot d'adresses à partir d'un même identifiant
- Avec stockage :
  - 64 bits de poids faible du hash de la valeur précédente ou aléatoire, bit U/L = 0
  - ne doit pas être une valeur réservée puis sauvegarde dans la table
- Sans stockage :
  - aléatoire uniquement, peut utiliser un historique
  - source d'aléas similaire à RFC 7217

Comment palier la perte de confidentialité ? (3)

- *Adresse MAC connue globalement*
- *Pistage et analyse possible (adresse non variable)*

Privacy extensions in SLAAC (RFC 4941)

- Adresses temporaires
  - durée de vie inférieure à certains paramètres
  - association d'un CREATION_TIME
  - ajout de l'IID
  - fonction DAD obligatoire