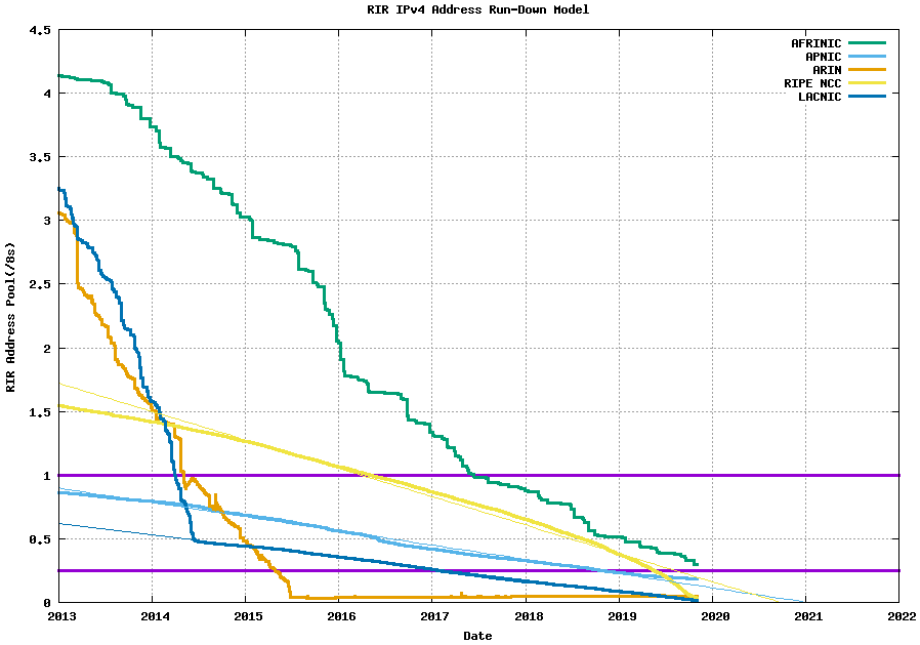
93 - Migration de l'infrastructure d'un établissement en double pile IPv4 / IPv6

Jérôme BERTHIER / Guillaume CASSONNET – Inria – DSI

01

Pourquoi IPv6 ?



Source Potaroo – 04/11/2019
http://www.potaroo.net/tools/ipv4/index.html

- Épuisement IPv4 global
- Conséquences à terme :
  - Frein au développement Internet
  - Dégradation de l'usage (CGN…)
- Être « acteur » de cette transition
  - Connectivité des utilisateurs
  - Présence Internet des services

Constats positifs

- **IPv6 présent chez les FAI et les fournisseurs de services**
- **IPv6 disponible techniquement « partout » (réseau, système…)**
- **IPv6 disponible sur RENATER depuis 2002 !**
- **IPv6 actif par défaut sur les systèmes !**
- **Choix à faire**
  - Ne rien faire mais induire une dette technique et impacter la sécurité
  - Investir du temps pour désactiver le protocole (parfois impossible selon le service)
  - Mettre des moyens pour implémenter le protocole !
- **Sortir de la vision « IPv6 = coûts, difficultés… »**

02

Prérequis IPv6

Considérer IPv6 globalement !

- **Être soutenu pour s'y engager entièrement**
- **Double pile IPv4 / IPv6**
  - Différent d'une migration => IPv4 subsiste
  - IPv6 = nouveau composant
- **Mesurer les dépendances entre services existants (VPN, DNS…)**
- **Assurer la formation pour connaître le protocole IPv6**
- **Adapter les méthodes existantes (outillage, référentiels, docs…)**
- **Inclure IPv6 dans tout projet (pas forcément un réflexe)**

Adapter son SI et outils d'infra

- **Monitoring : mettre IPv6 au même niveau qu'IPv4**
  - Hôtes et tests Nagios à dupliquer
  - Archivage de flux équivalent Netflow v9 pour supporter IPv6
- **IPAM/DNS : pouvoir y gérer IPv6 (plan adressage, zones DNS…)**
  - Gestion initiale de ficher texte zones Bind via GIT/Puppet
  - Évolution depuis vers la solution phpIPAM / PowerDNS (Pierre Bénard – Inria - JRES 2017)
- **Orchestration système pour activer IPv6**
  - Adaptation des fichiers kickstart CentOS
  - Automatisation Puppet / Ansible pour fiabiliser les actions
  - GPO Windows
- **Gestion des filtrages pare-feux en double pile**

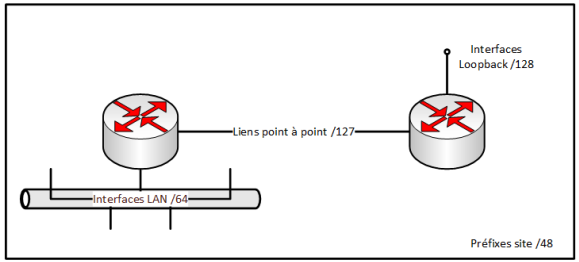
Allocation d'un préfixe IPv6 global

- **Demande auprès de notre LIR RENATER**
  - Peut prendre un peu de temps selon le cas
  - Attribution d'un préfixe /48 par site (65536 préfixes /64)
- **Coordination nécessaire avec le Réseau de Collecte selon le cas**
- **Plan d'adressage IPv6 à élaborer**
  - Grand espace « vierge »
  - Occasion de bâtir un modèle « neuf »
  - Oublier les « vieux » réflexes IPv4 (découpage au plus fin…)
  - Diverses méthodes documentées en ligne (celle proposée par SurfNet dans notre cas)

Plan d'adressage IPv6 retenu

- **Structure d'adressage « 2001:660:<network_id>:AGTT:: »**
  - A = allocation progressive par bloc /52 (site principal, site distant, expérimentation autonome…)
  - G = regrouper les réseaux « similaires » par bloc /56 (idéalement selon segmentation sécurité)
  - TT = provisionner 256 préfixes /64
  - Exemples réseaux fictifs :
    - Site principal / groupe DMZ / réseau WEB1 : *2001:660:<network_id>:1F01::/64*
    - Site distant / groupe UTILISATEURS / réseau PC10 : *2001:660:<network_id>:210A::/64*

- **Trois masques « standard » en production**
  - /128 pour les interfaces type Loopback
  - /127 pour les interconnexions directes point à point
  - /64 pour tout autre segment Ethernet



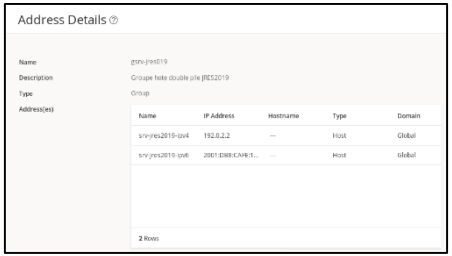
03

Déploiement IPv6

Infrastructure réseau

Routage et filtrage

- **Sécurité L3 :**
  - Filtrer les options « RH0 » et familles d'adresses IPv6 « anormales » (6Bone, RFC3849…)
  - Protéger des attaques de saturation de cache ND
- **Routage externe via peering BGP IPv6 (similaire à IPv4)**
- **Routage interne par ajout du protocole OSPFv3**
  - Réécriture d'OSPFv2 : transport en IPv6 uniquement, LSA différents
  - Exploitation similaire à OSPFv2
- **Filtrages pare-feu Juniper**
  - Aucune différence de traitement IPv4/IPv6 sur les équipements
  - Gestion des objets dupliqués dans l'outil d'administration sécurité
    - ➢ Un hôte IPv4 + un hôte IPv6 = un groupe par hôte double pile



Sécurité L2 – commutateurs Ethernet

- **Comme en IPv4, besoin de protéger certaines attaques locales**
- **Utile même si aucun service IPv6 offert (car protocole actif sur le LAN!)**
- **Activation de certaines fonctions Cisco IPv6 « First Hop Security »**
  - Protection « RA guard » contre les annonces de routeurs malveillants ou erronés
  - Protection « DHCPv6 snooping » contre les serveurs DHCPv6 malveillants ou erronés
  - Protection « ND inspection » contre la pollution de cache de voisinage ND
  - Protection « IPv6 snooping » contre le DOS DAD et pour le suivi des adresses
- **Équivalent disponible chez certains constructeurs**
- **Activable partiellement avec des filtres « access-list » par port**

IPv6 FHS – IPv6 snooping

- **Analyse les messages ND et DHCPv6**
- **Maintient une table globale de correspondance IPv6/MAC/Port/VLAN**

```
switch1#show ipv6 neighbor binding
Binding Table has 94 entries, 94 dynamic
[…]
   IPv6 address                  Link-Layer addr Interface vlan prlvl  age   state    Time left
ND  FE80::D681:D7FF:FE52:6768          D481.D752.6768  Gi8/0/9    815  0005 6175mn DOWN      6334 s
ND  FE80::BA27:EBFF:FE74:EDD4          B827.EB74.EDD4  Gi7/0/45   810  0005   12mn STALE     86082 s
ND  FE80::B034:7AC2:A358:1986          98E7.F4ED.EBD6  Gi7/0/21   815  0005  127s  REACHABLE  185 s
[…]
```

- **Traçabilité syslog des entrées :**

```
Sep 27 14:49:26 commut001 296677: Sep 27 14:49:25.608 MET: %SISF-6-ENTRY_CHANGED: Entry changed
A=2001:DB8:CAFE:1F00:54DB:2B9:725A:1B5C V=32 I=Gi6/0/31 P=0005 M=685C.329A.DBB5
```

04

Déploiement IPv6

Activation des services
Connectivité utilisateurs

Activation d'un service en IPv6 1/2

- **Activer un préfixe IPv6 sur le VLAN**
  - Paramétrage d'une adresse IPv6 globale sur la passerelle Juniper
  - Pas d'annonce RA nécessaire
  - Redistribution OSPFv3 préparée en amont
- **Adapter les filtres pare-feu**
  - Mettre le préfixe IPv6 à équivalent du préfixe IPv4
  - Reproduire les défiltrages « génériques » appliqués au préfixe IPv4 (admin, supervision, icmp…)

Activation d'un service en IPv6 2/2

- **Processus sans impact IPv4**
- **Étapes pour un serveur et service existants**

1. Réserver l'adresse IPv6 du serveur dans l'IPAM. *Pas de déclaration DNS à ce stade !*
2. Adresser en IPv6 l'interface du serveur
3. Configurer le service pour écouter et traiter IPv6 (voir l'article JRES pour les détails ☺)
4. Faire une recette de la connectivité IPv6 au serveur et au service (depuis un client privilégié)
5. Ajuster les filtres pare-feu pour IPv6 afin de refléter les accès IPv4 existants
6. Intégrer l'adresse IPv6 du serveur ou service aux tests de supervision
7. Déclarer l'adresse IPv6 du serveur ou service sur le DNS faisant autorité. *It works !*
8. Mettre à jour les documentations et référentiels concernant le service

Connectivité IPv6 utilisateurs 1/2

- **Choix de la méthode SLAAC**
  - Simplicité !
  - Auto configuration sans état
  - Identifiants d'interface « non prédictibles » mais pouvant être « stabilisés » (RFC 7217)
  - DNS resolver (transport IPv4) annoncés via DHCPv4
- **Traçabilité de l'auto-adressage via les logs binding FHS**
- **Communiquer les préfixes IPv6 aux partenaires ou fournisseurs**
  - Adaptation des défiltrages pour équivalent IPv4
  - Adaptation des services pour équivalent IPv4

Connectivité IPv6 utilisateurs 2/2

- **Processus sans impact IPv4**
- **Étapes pour un VLAN utilisateur**

1. Redistribution OSPFv3 préparée en amont
2. Activer un préfixe global IPv6 sur la passerelle du VLAN. *Ne pas activer d'annonces RA à ce stade !*
3. Adapter les filtres pare-feu IPv6 pour équivalent du préfixe IPv4
4. Faire une recette de la connectivité IPv6 depuis un client configuré avec une IPv6 statique
5. Activer les annonces RA sur la passerelle Juniper. *It works !*

```
set protocols router-advertisement interface reth0.32 prefix 2001:DB8:CAFE:32::/64
```

05

Bilan et perspectives IPv6

Cohabitation IPv4/IPv6

- **Perturbation possible si IPv6 dysfonctionne**
- **Algorithme « Happy Eyeballs » RFC 6555**
  - Permet de palier au problème sur un des deux protocoles (choix IPv6 ou du plus rapide en théorie)
  - Pas implémenté dans toutes les applications (navigateurs Web compatibles)
  - Clients Linux mount et openssh gèrent mal une rupture IPv6 : lenteur ou absence de repli IPv4
- **Ne pas publier un enregistrement DNS IPv6 si non joignable !**
- **Attention aux services double pile conditionnés par listes IPv4 source !**

Une expérience concluante

- **Trafic IPv6 WAN actuel : 13,2 % entrant / 9,3 % sortant**
- **Impact maitrisé sur le support informatique**
- **Chemin long par manque de priorisation « officielle »**
  - Août 2007 : assignation du préfixe /48 du site
  - Fin 2007 : activation peerings BGP RENATER et REAUMUR
  - Février 2013 : firewall externe Cisco – activation inspection IPv6
  - Mars 2013 : déploiement WAN redondant - routage dynamique OSPFv3
  - Janvier 2014 : déploiement IPv6 Cisco sur le VLAN des administrateurs Service Informatique
  - Juin 2014 : déploiement IPv6 pare-feux Juniper
  - Novembre-Décembre 2015 : déploiement sécurité L2 Cisco IPv6 « First Hop Security »
  - Juin-Octobre 2018 : déploiement connectivité IPv6 utilisateurs et activation IPv6 des services

Évolutions

- **Porter la problématique de manière globale pour l'institut (formations)**
- **Activer les services « faciles »**
  - Connectivité IPv6 utilisateurs Wifi
  - Présence et connectivité VPN SSL utilisateurs
- **Mais de gros chantiers à venir**
  - Déploiement transverse d'un service L3VPN RENATER IPv6
  - Qualification de « load balancer » IPv6
  - Qualification de « multi homing » BGP RENATER IPv6
  - Qualification adressage IPv6 global sur Active Directory
- **In fine, inclure réellement IPv6 partout !**

Merci !

Suivez-nous sur www.inria.fr