Quelques points non résolus d'IPv6

Matthieu Herrb
CNRS-LAAS

JTR 2008, Vandoeuvre-Les-Nancy, 2-4 Juin 2008

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Introduction

- La transition vers IPv6 est inéluctable
- La question c'est quand ?
- Un certain nombre de difficultés subsistent :
  - fantasmes marketing
  - problèmes techniques
- Écouter aussi les sceptiques à propos d'IPv6

Motivations

Mon implication dans IPv6 :

- Né de mon activité pour XFree86 et OpenBSD
  $\longrightarrow$ patches IPv6 pour X (avec Itojun)
- plus tard : projet Remip $\longrightarrow$ déploiement de services IPv6 au LAAS.

Difficultés rencontrées dans ces deux projets
$\longrightarrow$ papier JRES 2005.

Depuis cette présentation :

- beaucoup d'intérêt pour le sujet
- quelques évolutions en pratique
- beaucoup reste à faire

Support effectif pour les utilisateurs

But : arriver à fonctionner correctement indifféremment :

- en IPv4 seul,
- avec une double pile,
- en IPv6 seul.

Nécessite plusieurs éléments :

- Niveau infrastructure : supporter les 2 protocoles à tous les niveaux : routage, firewalls, management (SSH, SNMP), sur les serveurs et les équipements actifs.
- Niveau système d'exploitation des postes utilisateurs : configuration des interfaces, routage, firewall local, etc...)
- Niveau applicatif : supporter le protocole dans tous les composants de toutes les applications.

Le tout sans devoir restreindre le choix des fournisseurs.

Avertissements

- Je ne suis pas un spécialiste d'IPv6
- Je ne travaille pas chez un fournisseur d'accès réseau
- Les réseaux que j'utilise/administre ne font rien de très compliqué
- Je suis développeur d'OpenBSD et membre du CA de la fondation X.Org

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Complexité

Pour l'utilisateur :

- Adresses 128 bits : trop lourd à manipuler manuellement
- Erreurs de transcription : DNS,..
- Interfaces réseau multiples, adresses multiples : risques d'erreur (sécurité)

Pour le réseau :

- Explosion des tables de routage, solutions ?
- Multiplication des passerelles (6to4, teredo, etc...)
- Multi-homing IPv6 ?

Stabilité

Deux ans entre la sortie d'un RFC et la disponibilité du composant logiciel dans les produits commerciaux...

- nombreux composants encore expérimentaux
- certains aspects (auto-configuration DNS – RFC5006) encore en cours de discussion.

$\longrightarrow$ environnement pas encore favorable à des déploiements commerciaux

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Le schéma ~~de migration~~ d'intégration classique

Basé sur la double-pile

- obtenir un espace d'adresse IPv6
- rendre cet espace disponible sur le réseau local et connecté à l'extérieur
- déployer des clients et des services dans cet espace

Espace IPv6

Peu d'opérateurs fournissent une infrastructure IPv6 native.
Encore souvent « expérimentale » donc :

- utilise des tunnels divers et variés (Teredo, 6to4, etc..)
- routes IPv6 en moyenne plus longues
- utilise du matériel de 2nde classe
- instabilité des normes : problèmes d'interopérabilité
- moins bien supervisé : pannes durent plus longtemps
- traitements moins prioritaires

Réseau

- Nécessité PMTU fonctionnel : ne pas filtrer trop d'icmpv6
- Problèmes observés en pratique (solution : diminuer le MTU sur les interfaces en bout ?)
- Rogue routeurs Windows

DNS

- Toujours pas de résolution inverse dans bien des cas.
- Problème des adresses link-local
- Réponses incorrectes aux requêtes AAAA :
  - enregistrement ’A’
  - trou noirs : pas de réponse ou erreur NXDOMAIN,
  - réponse AAAA mais service non accessible.
- Quelques restes de la zone `ip6.int`
- Quelques clients/serveurs/firewalls qui ignorent l’extension EDNS0
  $-> $ bloquent certaines réponses trop longues ($>$ 512 octets).

DHCP et accès au réseau

Auto-configuration IPv6 $\longrightarrow$ configuration des serveurs DNS ?
Une solution : DHCPv6.
Mais :

- Serveurs peu répandus (Wide DHCPv6, ...)
- Intégration du client dans les systèmes ?
- Plus généralement : manque de souplesse dans la configuration d'IPv6 dans les systèmes.
  - **Bien :** pas de boutons inutiles pour les novices
  - **Pas bien :** config par défaut parfois (souvent) inadaptée.
- Encore plus généralement : IEEE802.1X, WPA, etc. en environnement IPv6 ?

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Double pile - conséquences

- Plusieurs adresses pour un service
- Comment choisir la bonne ?
- Pas de mécanisme standard
- Politique noyée dans les applications
  - dans les fichiers de config
  - dans le code lui-même
  - souvent IPv6 d'abord, IPv4 en backup
- Conséquences sur la performance :
  - Délais pour échec IPv6 -> backup sur IPv4 très lent.
  - d'où recommandation : désactiver v6 :-(

Ce qu'il faudrait

Un outil de définition de la politique

- globale pour un système
- pour un utilisateur

Définit :

- l'ordre de préférence entre les protocoles
- des exceptions (pour traiter les problèmes évoqués plus haut)
- éventuellement un mécanisme adaptatif (apprentissage)

Pour les connexion sortantes et entrantes.
Peut influencer l'ordre des adresses retournées par `getaddrinfo()`.

Applications

Depuis 2005 pas mal de progrès dans les applis de base

- Samba : version 3 supporte IPv6
- Squid : Patches IPv6 enfin intégrés
- NFS (hors de Solaris)
- reste quelques problèmes :
  - pas de NetBIOS ipv6 : config par défaut samba ne supporte pas v6
  - lourdeur logicielle : serveurs IPv6 plus gourmand (ex. Filer ne tient pas la charge si IPv6 activé, dixit leur hot-line)

Adresses IPv4 mappées dans IPv6

Fausse bonne idée pour la transition.
Principe : un socket IPv6 (Address family AF_INET6) accepte aussi des connexions IPv4. Mappe les adresses sous la forme :ffff :a.b.c.d.

- théoriquement interdit de transporter ces adresses. Qui le garanti ?
- introduit une forme d'adressage de plus
- filtrer explicitement ces adresses.
- gérer explicitement 2 sockets

Messagerie

LAAS : double pile SMTP depuis début 2005.

Quelques connexions échouent :

- mauvaise négociation PMTU → perte de fragments → timeouts TCP
- certains clients basculent en v4 d'autres restent bloqués sur l'adresse v6.
- serveurs distants avec IPv6 configurés mais pas de route vers l'extérieur : échec connexion IPv6 -> considérée comme fatale.
- récemment chez un gros industriel de la région :

```
RCPT TO : matthieu.herrb@laas.fr
451 IPv6 not supported
```

Résultat : installation d'un 3e MX sans IPv6 !

Téléphonie sur IP

A priori la téléphonie sur IP est fortement intéressée par IPv6 :

- protocoles (SIP, H.323) nécessitant une connexion de bout en bout
- gros consommateur d'adresses IP

Expérience LAAS : aucun prestataire ayant répondu à notre appel d'offre (qui citait IPv6) ne supporte IPv6 dans ses solutions.

Cisco propose un Beta-test.

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Sécurité

- Complexité du filtrage
  - ne pas oublier d'adresse possible
  - format des paquets $\longrightarrow$ problèmes d'implémentation
- Failles dans le protocole (ex. HDR0 routing header) ?
- Failles dans l'implémentation non encore découvertes (quelques corrections préventives dans OpenBSD récemment) ?
- Peu (pas) d'IPSec avec IPv6 en pratique (pbs IKE)
- Fuites d'infos (adresse MAC) via l'auto-configuration + ICMPv6 ouvert
- IPv6 n'est pas la fin du NAT... (tunnels,...)

Avantage : scans quasi impossibles

Plan

1 Introduction

2 Au niveau du protocole

3 Défauts liés au déploiement

4 Applications

5 Sécurité

6 Conclusions

Après la double pile ?

Face à la pénurie annoncée des adresses IPv4, la double-pile n'est pas la solution...

Il faudra un jour des systèmes sans IPv4.

- $\Rightarrow$ compléter l'offre des outils capables de faire de l'IPv6,
- $\Rightarrow$ renforcer les tests en environnement IPv6 seul.

Conclusion

- Aujourd’hui sans motivation définie : urgent d’attendre
- Attention au mythe de la double-pile
- Solutions concrètes pour un déploiement natif ?
- Dépend aussi du bon-vouloir du « marché »...

Bibliographie

- IPv6 : It's time to make the move, Mark Kosters and Megan Kruse, ;login :, volume 33 numero 2, avril 2008.
- Are Commercial Firewalls Ready for IPv6 ?, David Piscitello, ;login :, volume 33, numéro 2, avril 2008.
- IPv6 Transition & Operational Reality, Randy Bush, NANOG Albuquerque, octobre 2007. http://www.nanog.org/mtg-0710/bush.html
- PANEL : Pragmatismv6 : A Grown-up, Critical Examination of IPv6, NANOG, octobre 2007, http://www.nanog.org/mtg-0610/underwood.html
- IPv6 Routing Headers Security Philippe Biondi and Arnaud EBALARD, CanSecWest 2007, Vancouver Mai 2007. http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf