IPv6 : fonctionnement et déploiement

Olivier Togni

Université de Bourgogne

IEM/LE2I

www.u-bourgogne.fr/o.togni

olivier.togni@u-bourgogne.fr

modifié le 04/10/2017

Ressources bibliographiques

- IPv6 Théorie et pratique 4ed, *G. Cizault, O'Reilly 2005*
  (version en ligne avec mises à jour sur http://livre.g6.asso.fr*)*
- The Second Internet - Reinventing Computer Networking with Ipv6, 2010, Lawrence E. Hughes, en ligne à http://www.infoweapons.com/content/free-ipv6-book-second-internet
- IPv6: Theory, Protocol, and Practice, 2nd ed, *P. Loshin, Elsevier, 2004*
- www.urec.fr Tutoriel IPv6 de B. Tuy
- www.ietf.org RFC 2460, ...

Historique

- En 1992, constat de
  - Pénurie des adresses
  - Augmentation des tables de routages

  => Projet IP new generation (IPng)
- En 1995, RFC 1883: «Internet Protocol version 6»
- Depuis, de nombreuses modifications et normes complémentaires

Adresses

2^128 = 3,4*10^38 adresses disponibles

Sur 128 bits : 8 mots de 16 bits séparés par des « : »

Ex: 3201:001A:12FF:0000:0000:0000:FFFE:8ABC

:: pour abréger plusieurs mots nuls consécutifs

Ex: 3201:1A:12FF::FFFE:8ABC

3 types d'adresses: unicast, anycast, multicast

=> plus de broadcast!

Utilisent les principes de CIDR: adresse/longueur_préfixe

Ex: 2001:660:3003::/48

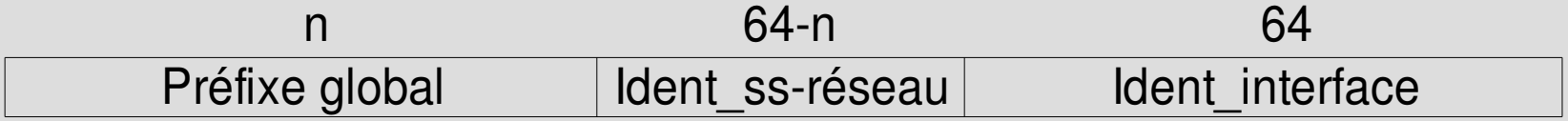
Espace d'adressage (iana.org)

INTERNET PROTOCOL VERSION 6 ADDRESS SPACE
(last updated 2008-05-13)

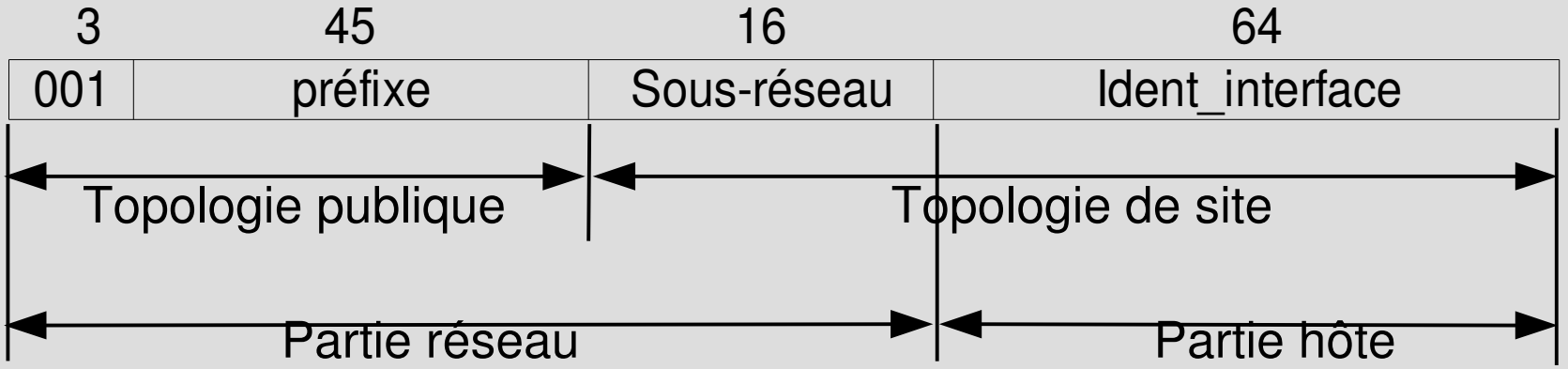
IPv6 Prefix	Allocation	Reference
0000::/8	Reserved by IETF	[RFC4291]
0100::/8	Reserved by IETF	[RFC4291]
0200::/7	Reserved by IETF	[RFC4048]
0400::/6	Reserved by IETF	[RFC4291]
0800::/5	Reserved by IETF	[RFC4291]
1000::/4	Reserved by IETF	[RFC4291]
2000::/3	Global Unicast	[RFC4291]
4000::/3	Reserved by IETF	[RFC4291]
6000::/3	Reserved by IETF	[RFC4291]
8000::/3	Reserved by IETF	[RFC4291]
A000::/3	Reserved by IETF	[RFC4291]
C000::/3	Reserved by IETF	[RFC4291]
E000::/4	Reserved by IETF	[RFC4291]
F000::/5	Reserved by IETF	[RFC4291]
F800::/6	Reserved by IETF	[RFC4291]
FC00::/7	Unique Local Unicast	[RFC4193]
FE00::/9	Reserved by IETF	[RFC4291]
FE80::/10	Link Local Unicast	[RFC4291]
FEC0::/10	Reserved by IETF	[RFC3879]
FF00::/8	Multicast	[RFC4291]

Plan d'adressage global

RFC 3587 rend obsolète l'adressage agrégé



Par exemple:



Identifiant d'interface

Identifiant sur 64 bits pour désigner une interface connectée sur un lien

Peut être construit à partir de l'adresse de niveau 2 de l'interface réseau:

- EUI-64 (firewire, 802.15.4) : inverser le 7ième bit
- MAC-48 (Ethernet, Wifi, FDDI) : ajout de FFFE au milieu et inversion du 7ième bit => identifiant unique au niveau mondial
- Si pas d'adresse de niveau 2=> nombre au hasard ou saisie manuelle

Adresses unicast globales

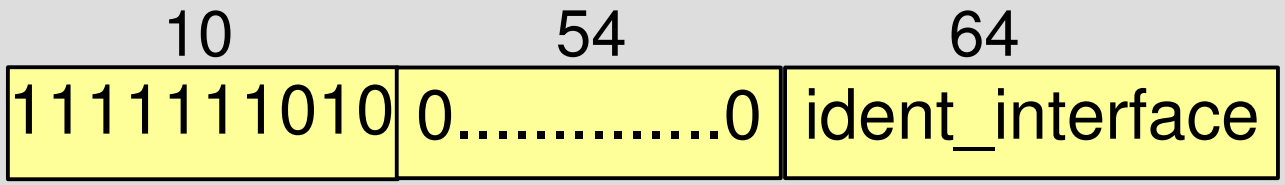
IPV6 GLOBAL UNICAST ADDRESS ASSIGNMENTS [last updated 2008-05-13]

Global Unicast Prefix	Assignment	Date			
2001:0000::/23	IANA	01 Jul 99	2001:4800::/23	ARIN	24 Aug 04
2001:0200::/23	APNIC	01 Jul 99	2001:4A00::/23	RIPE NCC	15 Oct 04
2001:0400::/23	ARIN	01 Jul 99	2001:4C00::/23	RIPE NCC	17 Dec 04
2001:0600::/23	RIPE NCC	01 Jul 99	2001:5000::/20	RIPE NCC	10 Sep 04
2001:0800::/23	RIPE NCC	01 May 02	2001:8000::/19	APNIC	30 Nov 04
2001:0A00::/23	RIPE NCC	02 Nov 02	2001:A000::/20	APNIC	30 Nov 04
2001:0C00::/23	APNIC	01 May 02	2001:B000::/20	APNIC	08 Mar 06
2001:0E00::/23	APNIC	01 Jan 03	2002:0000::/16	6to4	01 Feb 01
2001:1200::/23	LACNIC	01 Nov 02	2003:0000::/18	RIPE NCC	12 Jan 05
2001:1400::/23	RIPE NCC	01 Feb 03	2400:0000::/12	APNIC	03 Oct 06
2001:1600::/23	RIPE NCC	01 Jul 03	2600:0000::/12	ARIN	03 Oct 06
2001:1800::/23	ARIN	01 Apr 03	2610:0000::/23	ARIN	17 Nov 05
2001:1A00::/23	RIPE NCC	01 Jan 04	2620:0000::/23	ARIN	12 Sep 06
2001:1C00::/22	RIPE NCC	01 May 04	2800:0000::/12	LACNIC	03 Oct 06
2001:2000::/20	RIPE NCC	01 May 04	2A00:0000::/12	RIPE NCC	03 Oct 06
2001:3000::/21	RIPE NCC	01 May 04	2C00:0000::/12	AfriNIC	03 Oct 06
2001:3800::/22	RIPE NCC	01 May 04			
2001:3C00::/22	RESERVED	11 Jun 04			
2001:4000::/23	RIPE NCC	11 Jun 04			
2001:4200::/23	AfriNIC	01 Jun 04			
2001:4400::/23	APNIC	11 Jun 04			
2001:4600::/23	RIPE NCC	17 Aug 04			

Adresses locales

Adresses lien local (link local): adresses dont la validité est restreinte à un lien

Forme: FE80::+ident_interface



Utilisées par les protocoles de configuration d'adresse globale, de découverte de voisins (neighbor discovery) et de découverte de routeurs (router discovery).

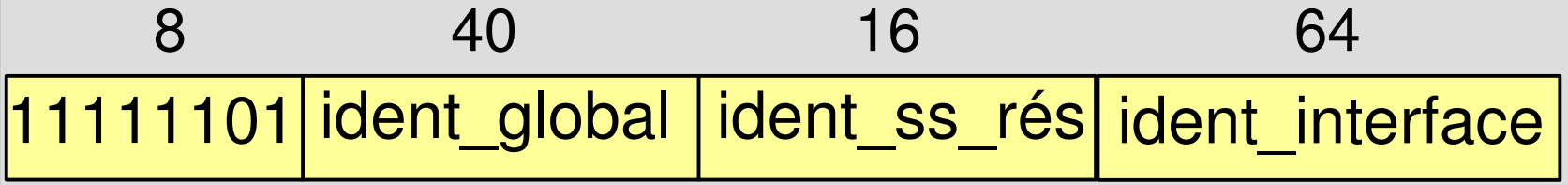
Le protocole de détection de duplication d'adresse (DaD) permet de s'assurer de l'unicité au niveau du lien.

Pas forwardées par les routeurs => usage local au lien

Adresses locales

Adresses unique local (ULA: unique local address):
Pour utilisation au sein d'une zone limitée (site ou entre un nombre limité de sites)

FC00::/7+bit à 1+ident_global+ident_sous_réseau+ident_interface



Ident_global généré pseudo-aléatoirement

Adresses prédéfinies

Adresses spéciales

- adr indéterminée: 0:0:0:0:0:0:0:0 ou bien ::
- adr de bouclage: ::1

Pour transition IPv4/v6:

- adr Ipv4 mappées: ::FFFF:a.b.c.d où a.b.c.d est une adr Ipv4
- adr Ipv4 compatibles: ::a.b.c.d => dépréciées (cf. RFC 4291)

Adresses multicast prédéfinies:

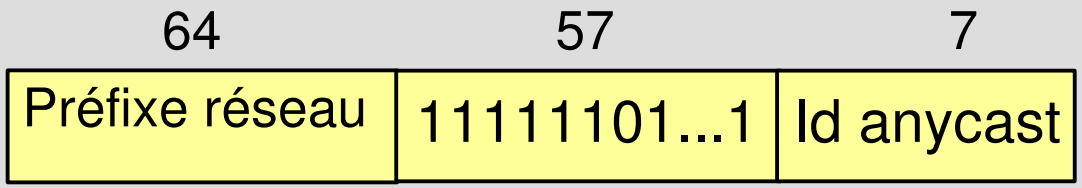
- FF02::1 => tous les noeuds Ipv6 sur le même lien local
- FF05::2 => tous les routeurs Ipv6 du site
- FF0E::101 => tous les serveurs NTP sur l'Internet

Adresses anycast

Une adresse anycast identifie un ensemble d'interfaces: un paquet à destination d'une adr anycast doit être acheminé par le réseau vers l'une des interfaces (la plus proche)
=> implémentation délicate, réservées pour les routeurs
Ex: serveurs FTP avec adresse générique

Ne peut être distinguée d'une adresse unicast (même plage d'adresses 2000 ::/3)

Adr anycast d'un sous-réseau: préfixe réseau+ 0...0
=> paquet transmis à cette adr doit être traité par l'un des routeurs du réseau
Adr anycast prédéfines (sur un réseau) : les 128 identifiants les plus grands



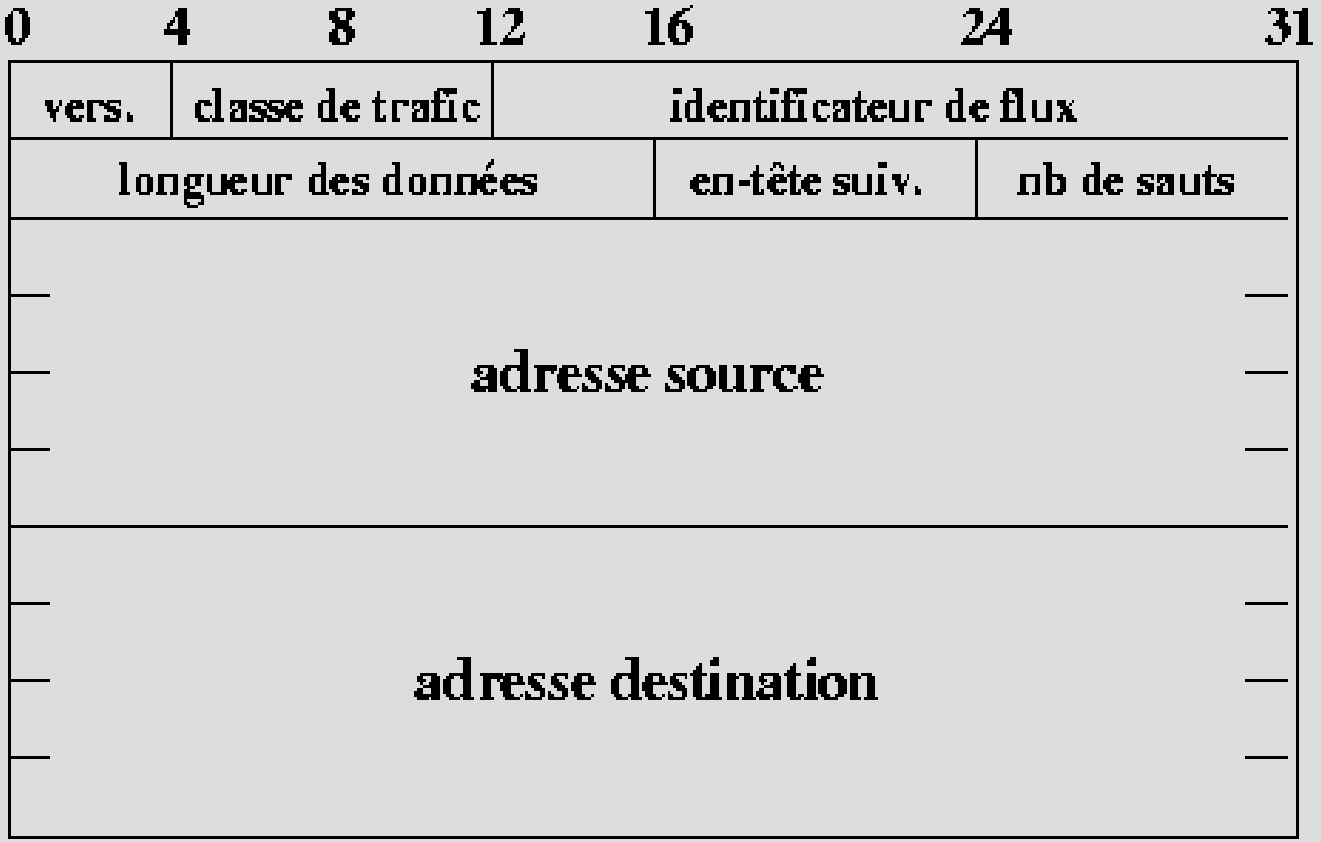
Exemple sous Linux

```
eth0    Link encap:Ethernet  HWaddr 00:0D:56:01:13:C9
        inet addr:193.52.237.96  Bcast:193.52.237.255  Mask:255.255.255.0
        inet6 addr: 2001:1111::20d:56ff:fe01:13c9/64 Scope:Global
        inet6 addr: fe80::20d:56ff:fe01:13c9/64 Scope:Link

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host

sit0    Link encap:IPv6-in-IPv4
        NOARP  MTU:1480  Metric:1
```

Format des datagrammes IPv6



=> 40 octets d'en-tête sans les options (5 mots de 64 bits)

Format des datagrammes IPv6

Version=6 (même champs que Ipv4)

Classe de trafic = champs type de service d'IPv4

Identificateur de flux: pour qualité de service, référence le contexte de la communication

Longueur des données: taille des données sans l'en-tête

En-tête suivant = champs protocole d'IPv4=soit protocole de niveau supérieur, soit numéro d'extension, les extensions contiennent ce champ pour chaînage

Nombre de sauts = TTL: décrémenté à chaque noeud traversé. Si 0, rejet et émission d'un message ICMP vers la source

Remarques

- Plus de champs Checksum car devait être ajusté par chaque routeur en raison du champ TTL modifié => les protocoles de niveau sup doivent mettre en place un ctrl d'erreur sur l'en-tête (étendue aux adr IP)
- Champs alignés sur mots de 64bits => optimisé pour architecture 64bits
- Moins de champs que dans Ipv4
- Entête de taille fixe => plus rapide
- Plus de souplesse dans les options

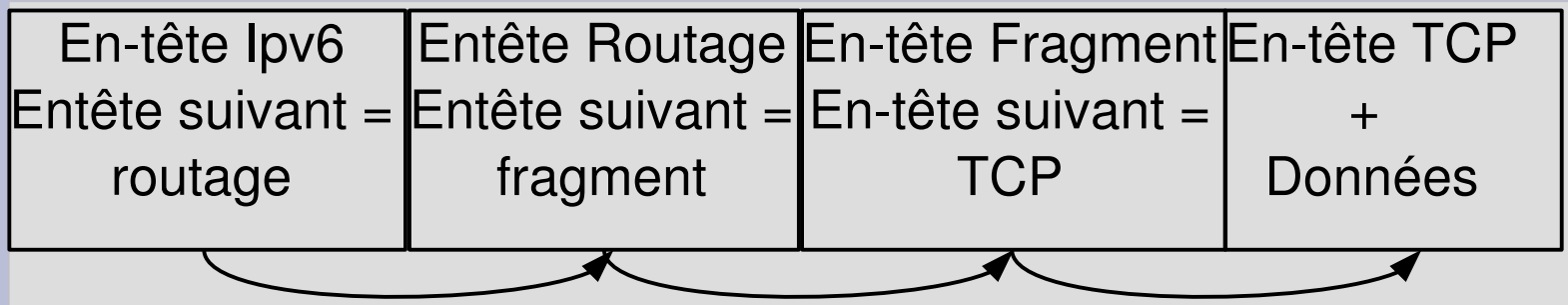
Extensions

Plus souples que les options d'IPv4, elles peuvent être chaînées entre elles et sont traitées seulement par les noeuds concernés

5 types d'extensions:

- Proche en proche (hop-by-hop)
  - toujours la première extension
  - remplace l'option Ipv4
  - analysée par chaque routeur
- Destination (traitée seulement par le destinataire)
- Routage
- Fragmentation
- Sécurité

Chaînage d'extensions



Champ En-tête suivant:

Proche en proche	0
Routage	43
Fragmentation	44
Confidentialité	50
Authentification	51
Fin des entêtes	59
Destination	60

TCP	6
UDP	17
IPv6	41
ICMPv6	58
SCTP	132
Mobilité	135
UDP-Lite	136

Protocoles associés à IPv6

ND (Neighbor Discovery): découverte des voisins

MLD (Multicast Listener Discovery)

- gestion des groupes multicast
- basé sur IGMPv2
- MLDv2 équivalent de IGMPv3 d'IPv4

ICMPv6 (Internet Control Message Protocol) :
«super» protocole qui

- couvre les aspects d'ICMPv4 (ctrl erreurs, ...)
- Transporte les messages ND et MLD

ICMPv6

Deux classes de messages (suivant le champs « type »):

- de 0 à 127 Messages d'erreur
- de 128 à 255 Messages d'information

Messages d'erreur les plus courants:

- Destination inaccessible (1)
- Paquet trop grand (2)
- Temps dépassé (3)
- Paramètre non reconnu (4)

Neighbor Discovery

Les noeuds Ipv6 sur un même lien utilisent ND pour:

- découvrir leur présence mutuelle
- déterminer l'adr de niveau liaison du voisin
- trouver les routeurs
- maintenir les infos sur l'accessibilité des voisins (NUD)

=> pas applicable aux réseaux NBMA (ATM, Frame Relay, ..)
car ND utilise le multicast

Synthèse de ARP, R-Disc, ICMP redirect

Neighbor Discovery

5 types de paquets ICMP:

- *Router Advertisement (RA)*: annonce périodique qui contient
  - liste des préfixes utilisés sur le lien
  - valeur possible du « nombre de sauts »
  - valeur du MTU

- *Router Solicitation (RS)*: l'hôte veut un RA immédiatement

- *Neighbor Solicitation (NS)*:
  - pour déterminer l'adr liaison d'un voisin
  - ou pour tester inaccessibilité
  - aussi pour tester duplication d'adr (DaD)

Neighbor Discovery

- *Neighbor Advertisement (NA):*
  - réponse à un paquet NS
  - avertir le changement d'une adresse physique

- *Redirect*: utilisé par un routeur pour informer un hôte d'une meilleure route

Résolution d'adresse

Au boot, l'hôte doit adhérer à 2 groupes multicast:

ff02::1 <=> tous les noeuds sur le lien

ff02::1:ffxx:xxxx adr de multicast sollicité (xxxxxx=24bits de poids faible de l'adr IPv6)

Résolution d'adresse:

1. Envoi paquet NS en multicast sollicité
2. L'hôte concerné répond par un message NA

Ex: @DST Ipv6	2001:0660:010A:4002:4421:21FF:FE24:87C1
Mult sol	FF02:0000:0000:0000:0000:0001:FF24:87C1
Ethernet	33-33-FF-24-87-C1

Auto-configuration

Seuls les routeurs doivent être configurés manuellement,
les hôtes peuvent obtenir leurs adresses automatiquement:

- Configuration sans état: la machine construit automatiquement ses adresses IPv6 en fonction d'informations qu'elle reçoit des routeurs
- Configuration avec état (contrôle de l'attribution des adresses): DHCPv6 (intérêt?)

Sécurité 1/3

IPsec: mécanismes de sécurité pour IP (v4 ou v6)
optionnel pour IPv4, obligatoire pour IPv6

L'extension d'authentification (AH : Authentication Header):
- s'assurer que l'émetteur du msg est bien celui qu'il prétend être
- contrôle d'intégrité pour garantir au récepteur que personne n'a modifié le contenu d'un message lors de son transfert sur le réseau

L'extension ESP (Encapsulating Security Payload):
- chiffrer l'ensemble des paquets ou leur partie transport et de garantir l'authentification et l'intégrité de ces paquets
- détecter les rejeux
- garantir (de façon limitée) la confidentialité du flux.

Sécurité 2/3

- IPv6 c'est IP => 95 % des problèmes de sécurité sont identiques à ceux d'IPv4
- Différences transitoires :
  - logiciels bogués, limités, lents,
  - administrateurs incompétents (mais attaquants aussi!),
  - techniques de transition complexes
- Différences de protocole :
  - Les annonces de routeurs (RA) ne sont pas sécurisées/authentifiées => solution SEND (secure ND)
  - Vie privée (@IPv6 dérivée de l'@MAC), scan des adresses, plus de NAT

Source : blog de Stéphane Bortzmeyer (AFNIC) http://www.bortzmeyer.org/

Sécurité 3/3

- Guides de sécurité pour le déploiement d'IPv6
  - Complet : recommandations du NIST pour un déploiement sécurisé
    Guidelines for the Secure Deployment of IPv6, Special Publication 800-119
    http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
  - De façon plus pratique : guide de l'UREC
    https://aresu.dsi.cnrs.fr/IMG/pdf/secu.articles.Archi.Securite.IPv6.pdf

Mécanismes de transition

A différents niveaux:

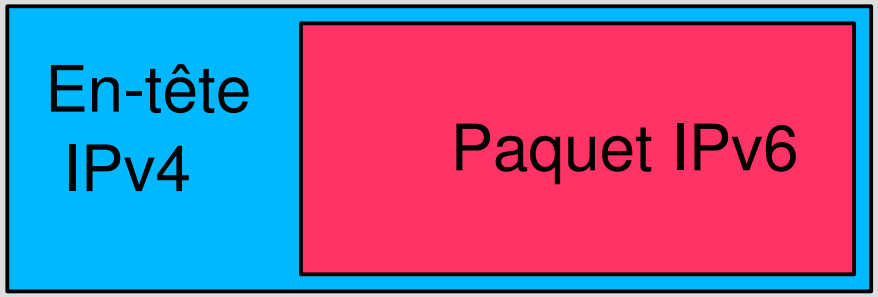
- Sur les hôtes: double pile
- Sur le réseau: tunnels
  - Manuels
  - Configurés: Tunnel Broker
  - Automatiques: TEREDO, 6to4, ISATAP, 6over4
- Par translation de protocoles
  - NAT-PT: traduire les en-têtes des paquets IPv6 en IPv4
  - Relais applicatifs: pour applications courantes

Hôte avec Double Pile

- L'hôte inclue les deux protocoles (IPv4 et IPv6) et chaque interface possède à la fois une adr IPv4 et une (ou plusieurs) adr IPv6
- Les applications fonctionnant avec IPv4 seulement utilisent IPv4, Les applications supportant IPv6 interrogent le DNS pour savoir si la destination possède une adr IPv6: si oui, l'hôte communique en IPv6; si non, IPv4 est utilisé
- => Facile à mettre en place mais ne réduit pas le besoin d'adresses et les deux types de réseaux sont complètement séparés

Tunnel IPv6-dans-IPv4

- Les paquets IPv6 encapsulés dans des paquets IPv4 à l'entrée du tunnel en ajoutant un en-tête IPv4 (avec champ PROTOCOLE=41) et décapsulés et traités comme s'ils provenaient du réseau IPv6 à la sortie du tunnel



- Les routeurs (ou hôtes) d'entrée et sortie du tunnel doivent être double pile
- Pour la couche v6: le tunnel est vu comme un une liaison v6 (un seul saut) et le réseau v4 comme une couche de niveau 2

Déploiement: applications

Peu de modifications sont en général nécessaires (sauf si l'application utilise les adresses)

- nouveau type de sockets en C: AF_INET6 au lieu de AF_INET
- pas de modification en Java grâce aux objets

Peu de services proposés en Ipv6 actuellement

(voir http://www.worldipv6launch.org/measurements/)

Déploiement: systèmes

- Windows: support de base depuis XP
  activation par « ipv6 install » sous DOS; activé par défaut sous Vista
- Linux: intégré depuis les noyaux 2.2
  les noyaux 2.6 gèrent l'IPsec
- BSD: IPv6 disponible depuis longtemps.
  Les version récentes proviennent de la souche KAME (japon)
- Macintosh: standard en MacOS X (10.3)

Déploiement: Réseau

- Routeurs (Cisco, juniper, 6wind ...): OK depuis plusieurs années
  - Après mise à jour de l'IOS pour certains
  - Présence de bugs
- Réseau: le coeur de l'Internet est compatible IPv6 SFINX: point d'échange Internet français géré par Renater intègre IPv6 depuis 2002

Déploiement: PMI-PME, ISP

Les plus frileux pour l'instant!

- Entreprises :
  - Changements coûteux
  - Pas de plus-value immédiate
- ISP : attendent la demande
  - Nerim: connexion ADSL IPv6 depuis 2003
  - Wanadoo: expérimentation depuis 2005
  - Free: proposé depuis décembre 2007
  - Orange : mise en place depuis 2016 sur fibre et VDSL

Conclusion

- Peine à s'imposer, mais la pénurie d'adresses IPv4 est maintenant une réalité
- Incitations gouvernementales : obligatoire pour les marchés (CEE et USA)
- Moyen d'interconnexion avec les mobiles en Asie
- IPv6 est-elle la bonne solution ?
  - RINA : Recursive InterNetwork Architecture → basé sur IPC
  - ...

… Qu'est-ce qu'on attend?