

Administration Système et Réseaux, Sécurité IPV6

Philippe Harrand

¹Département Informatique
Pôle Sciences et Technologies

²Direction Territoriale Sud Ouest
France Télécom

4 novembre 2007

IPV6

Généralités

Plan d'adressage

Auto configuration

Routage

Sécurité

Pourquoi changer ?

- ▶ Explosion d'Internet
- ▶ Pénurie d'adresses
- ▶ Flux temps réel
- ▶ Mais NAT

Objectifs

- ▶ Espace d'adressage ↑
- ▶ Tables de routage ↓
- ▶ Simplification du protocole
- ▶ Suppression des classes
- ▶ Sécurité ↑
- ▶ Type de service
- ▶ Multicast optimisé
- ▶ Portables
- ▶ ...

Migration

- ▶ Compatible avec couches supérieures
- ▶ Protocoles liés à IP
 - ▶ modifiés
 - ▶ ICMP, DHCP, DNS
 - ▶ ou supprimés
 - ▶ ARP
- ▶ Incompatibilité IPV4 ⇔ IPV6
- ▶ les routeurs doivent supporter les deux
- ▶ Problèmes mercantiles

Format datagramme

Version	Classe de trafic	Identificateur de flux	
Longueur des données	En-tête suivant	Nombre de sauts	
		Adresse IP source	
		Adresse IP source	
		Adresse IP source	
		Adresse IP source	
		Adresse IP destination	
		Adresse IP destination	
		Adresse IP destination	
		Adresse IP destination	
		Extensions optionnelles	
		Données	

Notation

- ▶ Notation hexadécimale
- ▶ "Bi-octets" séparés par ":"
- ▶ Les zéros non significatifs omis
- ▶ Les suites de zéros peuvent être condensées

Notation exemples

- ▶ 3FFE :BA98 :0000 :0000 :FEDC :BA98 :7654 :3210
- ▶ 3FFE :BA98 : :FEDC :BA98 :7654 :3210
- ▶ La longueur de la partie réseau (préfixe) systématiquement indiquée (presque)

Types d'adresses

- ▶ Unicast
Datagramme destiné à une machine unique
- ▶ Multicast
Datagramme destiné à plusieurs machines
- ▶ Anycast
Datagramme destiné à la machine la plus proche faisant fonctionner un service donné
- ▶ PAS DE BROADCAST

Unicast

- ▶ Portée globale (routable sur Internet) **2000/3**
le préfixe a une taille maximum de 64 bits
 - ▶ permanentes (2000 : :/16) allouées transitoirement avant l'ouverture du registre officiel.
 - ▶ permanentes (2001 : :/16) ouvertes à la réservation depuis 2001.
 - ▶ 6to4 (2002 : :/16) trafic IPv6 via un ou plusieurs réseaux IPv4.
 - ▶ 6bone (3ffe : :/16) expérimentation des interconnexions de réseaux IPv6.
 - ▶ Le reste réservé pour usage ultérieur.
- ▶ Portée limitée au segment de réseau (non routable) préfixe FE80/16
- ▶ Adresse de la machine : :1
- ▶ Adresse non spécifiée : :

Multicast

- ▶ Préfixe FF0X
 - ▶ X=1 portée noeud local
 - ▶ X=2 portée lien local
 - ▶ X=E portée globale
- ▶ Exemples
 - ▶ All-node-multicast sur lien local FF02 : :1
 - ▶ All-routers sur lien local FF02 : :2
 - ▶ All-DNS-servers FF0X : :FB
 - ▶ All-DHCP-servers FF05 : :1 :3
 - ▶ Neighbor Discovery FF02 : :1 :FF00

Anycast

- ▶ utilisées uniquement comme adresse de destination, pour s'adresser à un « service » « le plus proche »
- ▶ les routeurs traduisent les adresses *anycast* en adresses *multicast*
- ▶ un mécanisme de *heartbeat* permet à un routeur de connaître l'état de fonctionnement d'un service sur un lien donné
- ▶ les protocoles ospf et/ou bgp propagent (ou non) l'information
- ▶ les adresses anycast n'utilisent pas de préfixe spécial
- ▶ anycast est très utile pour la répartition de charge, la haute disponibilité et la résistance au deny de service

Partie hôte

- ▶ Laissée à l'appréciation de l'administrateur
- ▶ Globalement unique si 7^{ème} bit du premier octet à 1
- ▶ Souvent constituée à partir de l'adresse MAC et complétée à 64 bits (EUI64)

MAC address	00 :A0 :24 :E3 :FA :4B	24+24
EUI-64	02A0 :24FF :FEE3 :FA4B	24+40

le 7ème bit du premier octet est à 1 car l'unicité est garantie par l'IEEE

- ▶ Interface série ou interface virtuelle (PPP), sans adresse MAC, l'unicité n'est pas garantie. Ca ne pose pas de problème car ce sont des interfaces point à point. Le bit d'unicité restant à 0, on peut tout simplement les appeler FE80 ::1 et FE80 ::2 par exemple
- ▶ Utiliser l'adresse MAC unique dans l'adresse IPV6 permet de tracer l'activité d'une machine et ses déplacements (portable). Ce problème est contourné en autorisant la génération d'une partie hôte aléatoire (durée de vie très courte) pour toutes les connexions sortantes en conservant l'adresse unique pour les connexions entrantes.

Sans états

- ▶ Création adresse locale
 - ▶ Partie réseau : adresse "link-local" FE80/64
 - ▶ Partie hôte : adresse EUI-64
 - ▶ FE80 : :A0 :24FF :FEE3 :FA4B/64
- ▶ L'hôte émet une trame ICMPV6 de « sollicitation de voisin » en utilisant comme adresse de destination l'adresse de multicast formée de FF02 ::1 :FF00 ::/104 et des 24 derniers bits de son adresse EUI-64
- ▶ Toute machine dont les 24 derniers bits correspondent doit répondre en plaçant son adresse MAC dans la réponse
- ▶ Si OK, validation de l'adresse
- ▶ Adresse globale : attente sur l'adresse multicast all-nodes d'un paquet RA (Router Advertisement) contenant le préfixe global (10s)
- ▶ Possibilité d'émettre un message ICMPV6 de sollicitation de routeur à l'adresse multicast all-routers, message auquel les routeurs répondent par un message RA
- ▶ Vérification l'unicité de son adresse globale de la même manière que pour l'adresse locale.

Avec états

- ▶ DHCP V6 (RFC 3315) présente quelques différences par rapport à la V4
- ▶ Le client utilise son adresse link-local autoconfigurée comme adresse source et l'adresse multicast All_DHCP_Relay_Agents_and_Servers comme adresse destination
- ▶ Pour les autres différences, lisez la RFC 3315
- ▶ ddbler (<http://klub.com.pl/dhcpv6/>) fonctionne

ICMP V6

- ▶ Rôle plus important qu'en V4
- ▶ Gestion des erreurs (similaire à ICMP V4)
- ▶ Information
 - ▶ messages de diagnostic
 - ▶ messages pour la gestion des groupes multicast
 - ▶ messages de découverte de voisinage

ICMP V6

Type	Signification	Type	Signification
1	Destination Unreachable	131	Group Membership Report
2	Packet Too Big	132	Group Membership Reduction
3	Time Exceeded	133	Router Solicitation
4	Parameter Problem	134	Router Advertisement
128	Echo Request	135	Neighbor Solicitation
129	Echo Reply	136	Neighbor Advertisement
130	Group Membership Query	137	Redirect

Fragmentation

- ▶ La fragmentation nécessite des ressources importantes pour les routeurs
- ▶ Donc **PAS DE FRAGMENTATION** au niveau routeur
- ▶ MTU minimal fixé à 1280 octets (IP V4 \Rightarrow 576)
- ▶ Paquet trop gros détruit \Rightarrow ICMP "Paquet too big" avec MTU

Réseaux locaux

- ▶ Réseaux à 1 routeur
- ▶ RADVD
 - ▶ Répond aux messages de "Sollicitation de routeur"
 - ▶ Emet régulièrement des messages d'"Avertissement de routeur" (défaut $200 < T > 600$)
 - ▶ Ne pas émettre sur le "backbone"
 - ▶ Seule la "Passerelle par défaut" doit émettre
 - ▶ "Avertissement de routeur" contient :
 - ▶ adresse physique du routeur
 - ▶ information sur le préfixe
 - ▶ MTU (facultatif)

internets

- ▶ Statique
 - ▶ Comme IPv4
 - ▶ Mais adresses à rallonge !
- ▶ Dynamique
 - ▶ RIP \Rightarrow RIPng
 - ▶ OSPF \Rightarrow OSPFv3 (ospf6d pour quagga)
 - ▶ BGP \Rightarrow BGP

IPSEC intégré

- ▶ Dans les extensions
 - ▶ ESP (Encapsulating Security Payload)
 - ▶ AH (Authentication Header)
- ▶ Pas d'encapsulation des entêtes modifiés par le routage
- ▶ Mode "tunnel" ou "transport"
- ▶ On en reparle plus tard...