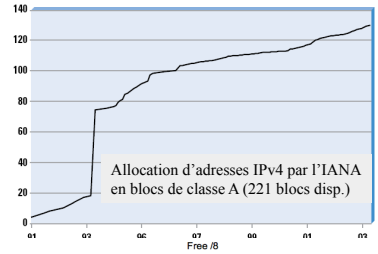
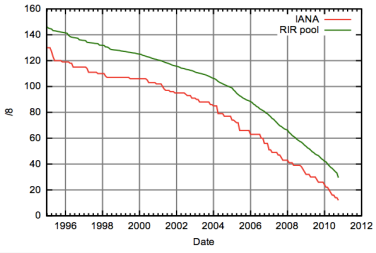
IPv6

- La nouvelle version du protocole IP
  - RFC 2460
- Pourquoi un nouveau protocole
  - Problèmes d'IPv4
    - Pénurie d'adresses
    - Croissance des tables de routage
    - Panoplie de protocoles autour d'IP
      - ARP pour chaque technologie sous-jacente
      - ICMP, IGMP
      - Mobilité (IP Mobile)
      - Sécurité (IPSec)

Pénurie d'adresses IPv4

- Mesures prises pour éviter l'épuisement des adresses
  - Adressage privé et NAT
    - Problèmes de compatibilité
      - Protocoles de sécurité
      - Applications multimédia
  - Allocation d'adresses classe C et routage CIDR
    - Permet une meilleure efficacité d'allocation d'adresse
- ➢ Pas d'épuisement, mais
  - Problèmes avec NAT
  - Problèmes d'efficacité d'IPv4 pour les réseaux à haut débit





Objectifs principaux d'IPv6

- Supporter des milliards d'ordinateurs, terminaux mobiles, …
- Réduire la taille des tables de routage
- Simplifier le protocole
  - Acheminement à haute vitesse
- Fournir une meilleure sécurité
- Permettre la mobilité d'ordinateurs
- Permettre au protocole une évolution future
- Permettre une coexistance entre IPv4 et IPv6
- Rester compatible avec les protocoles TCP, UDP, OSPF, RIP, BGP, DNS, ainsi qu'avec les applications

Historique

- RFC 1550: Appel de propositions pour IPng
- Déc. 1992: 21 propositions, 7 sélectionnées
- 3 propositions publiées et discutées
  - Deering (1993) : SIP: Simple Internet Protocol
  - Francis (1993) : Pip
  - Katz, Ford (1993) : TUBA: TCP et UDP sur CLNP (OSI)
- Combinaison et modification de SIP et Pip
  --> SIPP (SIP Plus) --> IPv6 (1995)

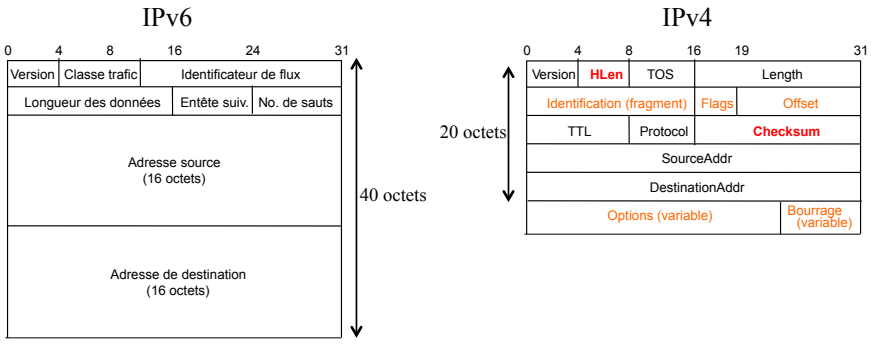
Survol des caractéristiques principales

- Adresses sur 128 bits au lieu de 32 bits dans IPv4
  - Adressage hiérarchique
- En-têtes simplifiés, peuvent être traités beaucoup plus rapidement!
  - Nombre de champs réduit de moitié
- Extensions des en-tête par des options
  - Traitement efficace des datagrammes par les routeurs
  - Introduction de nouvelles fonctionnalités (hop-by-hop, routage, fragmentation, destination, AH/ESP,….)
- Intégration d'éléments de sécurité
  - Authentification, intégrité, confidentialité
- Intégration de mécanismes de gestion de mobilité

Survol des caractéristiques principales

- Nouvelles fonctionnalités
  - Configuration automatique d'adresses
  - Routage par la source
  - Découverte de la MTU le long d'une route (IPv6 MTU et PMTU avec ICMPv6)
- La fragmentation n'est plus supportée par les routeurs
- ICMP, IGMP, ARP remplacés par ICMPv6

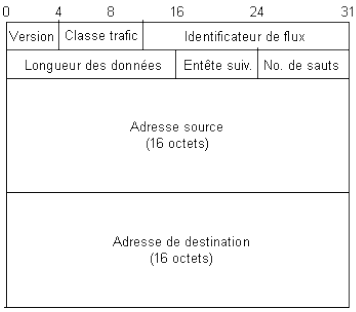
Format de l'en-tête de base



- Longueur fixe de l'en-tête
  - Header Length n'est plus nécessaire
  - Les en-têtes d'extensions sont utilisés pour des fonctionnalités optionnelles
- Le champs Checksum est éliminé pour des raisons d'efficacité
  - Le contrôle d'erreur à la couche Transport (TCP, UDP !) devient obligatoire

Les champs de l'en-tête

- Classe de trafic (8 bit)
  - Correspond au champs Type Of Service d'IPv4
  - Sera utilisé avec la sémantique des Services Différenciés
- Identificateur de flux (20 bit)
  - Normalisation pas encore terminée
  - Pourrait faciliter la classification des paquets d'une connexion
- Longueur des données (16 bit)
  - Indique la longueur des données qui suivent l'en-tête (contrairement au champs Longueur dans IPv4
  - Longueur maximale en mode normal: 65'535 octets
  - Option 'Jumbogrammes' pour des datagrammes plus longs
- En-tête suivant (8 bits)
  - Indique le type de l'en-tête qui suit
    - En-tête d'extension ou protocole de la couche supérieure
- Nombre de sauts
  - Similaire au champs Time-To-Live en IPv4 (1 à 65535)
  - Décrémenté de un à chaque pas jusqu'à zéro. Calculé rapidement puisque le routeur n'a pas à calculer le Checksum!



Utilisation du **TOS** pour la QoS avec IPv4

- DiffServ utilise les 6 bits du champ DS (Differentiated Services) pour classer les paquets
- Avec IPv6, les champs DS (DiffServ Code Point, DSCP: 6 bits)+ ECN (Explicit congestion notification, 2 bits: contrôle de congestion) remplacent le champ TOS de IPv4.
- Théoriquement 64 classes de trafic mais les RFC recommendent certains codages pour donner plus de flexibilité à l'opérateur pour définir ses classes de trafic.

Per-hop Behaviors

- La plupart des réseaux utilisent:
  - Default PHB (Per hop behavior)—qui est typiquement du trafic best-effort
  - Expedited Forwarding (EF) PHB—dédié au trafic « pertes faibles », « latence faible » (voix, vidéo, services en temps réel)
  - Assured Forwarding (AF) PHB—donne une assurance sur l'acheminement tant que certains débits ne sont pas dépassés (sinon utilisation de RED)
  - Class Selector PHBs—maintient une compatibilité avec le champ « precedence » (remplacé par DSCP) de IPv4.

Classes de trafic (RFC 4594)

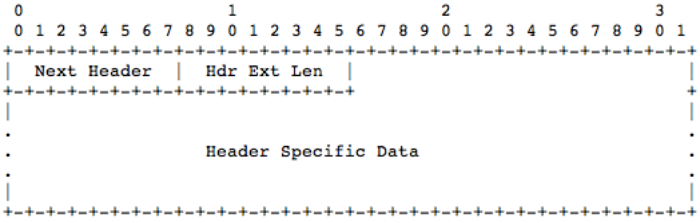
Application	L3 Classification			L2
	IPP	PHB	DSCP	Cos
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31	26	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

221048

www.cisco.com

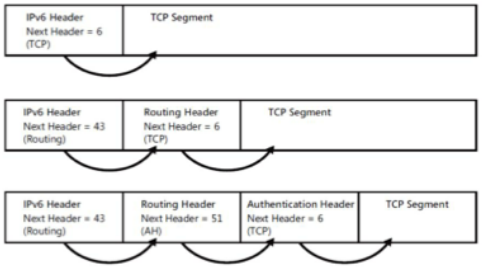
Les en-têtes d'extension

- Nouveau mécanisme remplaçant les options dans IPv4.
- Permettent d'implémenter des fonctionnalités supplémentaires
- Sont examinés par les systèmes terminaux (sauf en-tête hop-by-hop)
- L'entête d'extension (RFC 6564) a un champ « Next Header » (8 bits) puis « Header extension length » (8 bits) et « Header Specific Data » (de longueur variable, spécifique à l'entête d'extension) ou «Options»:



Les en-têtes d'extension

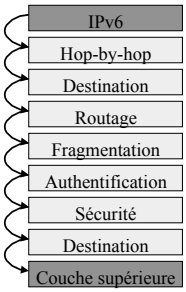
- Chaque en-tête indique l'en-tête suivant dans le premier champ (RFC2460)



Order	Header Type	Next Header Code
1	**Basic IPv6 Header**	-
2	**Hop-by-Hop Options**	0
3	**Destination Options (with Routing Options)**	60
4	**Routing Header**	43
5	**Fragment Header**	44
6	**Authentication Header**	51
7	**Encapsulation Security Payload Header**	50
8	**Destination Options**	60
9	**Mobility Header**	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Les en-têtes d'extension

- L'ordre de l'examen des en-têtes est important



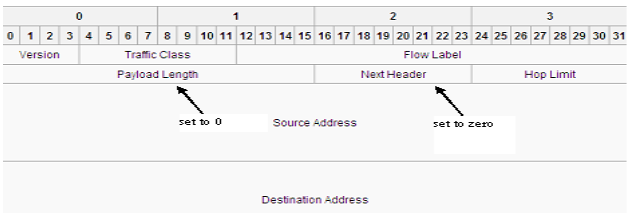
Examiné par chaque routeur intermédiaire. Utilisé pour les jumbogrammes.
Examiné par les router indiqué dans l'extension de routage
Liste de routeurs à traverser (Routage par la source)
Fragmentation et réassemblage par les systèmes terminaux
Authentification
Contient les données chiffrées du datagrammes
Examiné par le destinataire final du datagramme
P.ex. TCP, UDP

Entête **hop-by-hop**

- Toujours la première extension et doit être examinée par chaque nœud.
- Options (codées en TLV, type-length-value)
  - 0: Pad1
  - 1: PadN
  - 5: Router alert
  - 194: Jumbograms

Jumbogrammes

- Payload length + next header: remplir de 0!
- L'entête suivant sera du type « hop-by-hop »



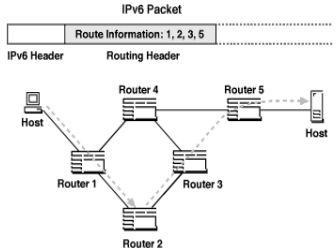
- Option type (8 bits): 0xC2
- Option length (8 bits): 0x04
- Option data: 32 bits jumbo payload length

Entête de destination

- Contient des informations optionnelles destinées à la destination
- Utilisé par Mobile IPv6 pour l'échange des messages d'enregistrement entre le nœud mobile (Mobile node) et le nœud à la maison (Home agent).

En-tête de routage

- Indique une séquence de routeurs qui doivent être traversés par le datagramme
- Permet de réaliser le routage par la source
  - Fonctionnalité existante déjà dans IPv4 mais peu efficace
- Algorithme
  - L'adresse destinataire du datagramme envoyé par la source est celle du premier routeur
  - Le premier 'destinataire' trouve l'adresse du prochain routeur dans l'en-tête de routage et la met comme prochain 'destinataire'
  - Chaque routeur décrémente la valeur du champ 'Segments restants'
- Plusieurs types de routage peuvent être définis



Format de l'en-tête de routage

0	8	16	31
En-tête suivant	Long. en-tête	Type de routage	Segm. restants
Réservé			
Adresse 1			
…			
Adresse N			

Fragmentation (rappel)

- La fragmentation nécessite un réassemblage à la destination. Problèmes potentiels:
  - Blocages
  - Les retransmissions vont aggraver l'encombrement du réseau
- La solution consiste à éviter la fragmentation avec « Path MTU discovery »
  - Découverte de la MTU la plus petite sur le chemin entre la source et la destination
  - Découverte du chemin (path MTU)

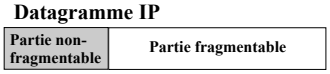
Path MTU discovery (RFC 1981)

- Méthode du « Path MTU discovery » (PMTU)
  - Le host source positionne le bit « Do not fragment » à 1 sur tous les datagrammes
  - Le nœud source commence par faire l'hypothèse que la MTU minimum est celle de l'interface sur lequel il envoie le datagramme
  - Les routeurs intermédiaires peuvent envoyer un message ICMP « destination unreachable/fragmentation needed » en cas de besoin. Ils ont l'interdiction de fragmenter un datagramme
  - Le host réduit l'estimation de PMTU et l'égale à la valeur communiquée par le message d'erreur ICMP

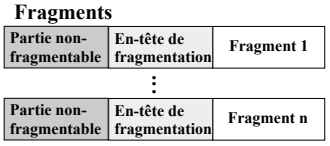
Fragmentation

- Contrairement à IPv4, la fragmentation est uniquement utilisée par la source du datagramme
- Chaque interface doit avoir une MTU d'au minimum 1280 octets
- Algorithme
  - Le datagramme originale est composé de deux parties
    - Partie non-fragmentable
      - En-tête IPv6 de base
      - Toutes les extensions à examiner par les nœuds intermédiaires
    - Partie fragmentable
  - Chaque fragment transmis comprend
    - La partie non-fragmentable
    - L'en-tête de fragmentation
    - Une partie du datagramme

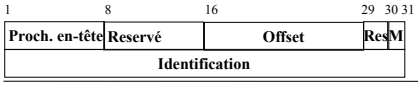
Datagramme IP



Fragments



Format de l'en-tête de routage



Technologie LAN/WAN	MTU IPv6
Ethernet II	1500
IEEE 802.11	2312
PPP	1500
Frame Relay (1592)	1592
ATM	9180

Adressage IPv6

- Adresses sur 128 bits (16 octets): 2^{128} adresses
  - Permet (théoriquement) d'adresser $3{,}4 \cdot 10^{38}$ interfaces
  - Environ 10^{28} adresses par personne sur la planète
  - Permet plusieurs niveaux hiérarchiques et une certaine flexibilité pour l'adressage et le routage.
  - Adresses locales (lien, site)
  - Adresse globale
- Notation
  - Sous forme binaire:
    - 1111101011011100 1010101101110101 0100001101000101 0100101001000101
    - 1010111100111111 0011001001010101 1111010000110001 1010010001001011
    - 8 groupes de 4 chiffres hexadécimaux, séparés par ':'
    - FADC:AB75:4345:4A45:AF3F:3255:F431:A44B
  - Les premiers 0 d'un groupe peuvent être omis
    - 123 au lieu de 0123
  - Compression des zéros: plusieurs groupes 0 peuvent être remplacés par '::'
    - 1080:0:0:0:0:800:200C:2342 --> 1080::800:200C:2342
    - 0:0:0:0:0:0:0:1 --> ::1
  - Suffixe en décimal pointé: les adresses IPv4 peuvent être écrit avec les 4 derniers octets en notation décimale
    - ::192.31.32.46

Découverte de IPv6 sur votre PC/Mac

- Pinguez votre adresse de loopback:

```
unknown00254bbd98c6:~ stephanrobert$ ping6 ::1
PING6(56=40+8+8 bytes) ::1 --> ::1
16 bytes from ::1, icmp_seq=0 hlim=64 time=0.127 ms
16 bytes from ::1, icmp_seq=1 hlim=64 time=0.086 ms
16 bytes from ::1, icmp_seq=2 hlim=64 time=0.089 ms
16 bytes from ::1, icmp_seq=3 hlim=64 time=0.092 ms
16 bytes from ::1, icmp_seq=4 hlim=64 time=0.088 ms
16 bytes from ::1, icmp_seq=5 hlim=64 time=0.167 ms
```

- Ou l'adresse IPv6 de votre voisin (dans le même réseau local que vous). Pour connaître son adresse: ifconfig

```
unknown00254bbd98c6:~ stephanrobert$ ping6 fe80::216:cbff:fe92:5cf7%en0
PING6(56=40+8+8 bytes) fe80::225:4bff:febd:98c6%en0 --> fe80::216:cbff:fe92:5cf7%en0
16 bytes from fe80::216:cbff:fe92:5cf7%en0, icmp_seq=0 hlim=64 time=483.840 ms
16 bytes from fe80::216:cbff:fe92:5cf7%en0, icmp_seq=1 hlim=64 time=0.658 ms
16 bytes from fe80::216:cbff:fe92:5cf7%en0, icmp_seq=2 hlim=64 time=0.660 ms
16 bytes from fe80::216:cbff:fe92:5cf7%en0, icmp_seq=3 hlim=64 time=0.609 ms
16 bytes from fe80::216:cbff:fe92:5cf7%en0, icmp_seq=4 hlim=64 time=0.655 ms
```


Préfixes IPv6

- La notion de classes a disparu (A,B,C,..) ainsi que celle du sous-réseau comme dans IPv4
- Rappel: adresse IP =<network ID><Host ID>. Tous les hosts du même LAN doivent avoir le même <Network ID>!
- Comment différencier la partie réseau de la partie « host »? C'est justement le rôle du préfixe
- Nous utilisons la notation de CIDR: ip-v6 address/longueur du préfixe.
  - Exemple: 2001:DB8::BA30:0:0:0:0/60
- Ici nous pouvons avoir des longueurs de préfixe jusqu'à /128.
- Exemples concrets (Swisscom IP-Plus):
  - 2001:918:fff8::/48 pour une route ou summary
  - 2001:918:fff8:ff0::/64 pour un sous-réseau
  - 2001:918:fff8:ffa::/126 pour un sous-réseau
  - 2001:918:fff8:fff::1/128 pour un nœud ou une adresse de loopback

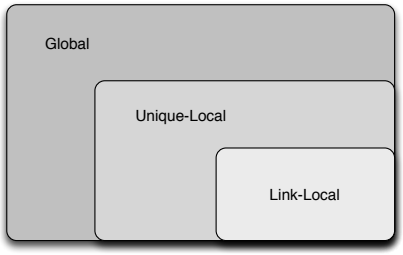
Espaces d'adresses actuellement alloués

- Types d'adresses
  - Adresses unicast
  - Adresses multicast
  - Adresses anycast
- Les adresses ont une durée de vie.
- Sans adresse broadcast
  - Diffusion peut être simulée par des adresses multicast

Préfixe	Type d'adresse	Fraction de l'espace d'adresses
0000 0000	**Réservé (compatible IPv4)**	**1/256**
0000 0001	Non affecté	1/256
0000 001	Adresses NSAP (OSI)	1/128
0000 010	Adresses Network IPX Novell	1/128
0000 011	Non affecté	1/128
0000 1	Non affecté	1/32
0001	Non affecté	1/16
001	**Adresses unicast globales agrégeables (RFC 2374)**	**1/8**
010	Non affecté	1/8
011	Non affecté	1/8
100	Non affecté (avant : adresses géographiques)	1/8
110	Non affecté	1/8
1110	Non affecté	1/16
1111 0	Non affecté	1/32
1111 10	Non affecté	1/64
1111 110	Non affecté	1/128
1111 1110	Non affecté	1/256
1111 1110 0	Non affecté	1/512
1111 1110 10	**Adresse locale unicast de lien**	**1/1024**
1111 1110 11	**Adresse locale unicast de site**	**1/1024**
1111 1111	**Adresses multicast**	**1/256**

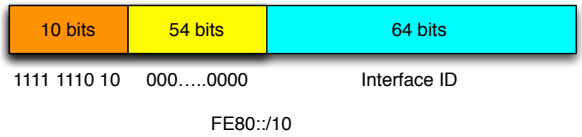
Type d'adresses

- Adresses Unicast
  - Link-local Unicast: signification locale uniquement. Pas routable en dehors du lieu local.
  - Unique local Unicast: signification locale. Pas routables sur Internet.
  - Global Unicast: routable à travers tout le réseau IPv6



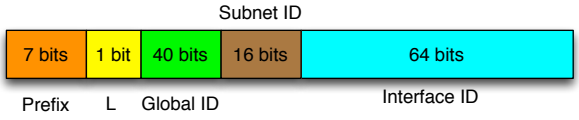
Adresses **Link-local Unicast** (RFC 3927)

- Structure extrêmement **simple**!
- Aucune possibilité de routage
- **Automatiquement assignée** dès que IPv6 est en fonction (pas d'autoconfiguration!)
- Utilisation limitée aux interfaces directement connectées sur le même 'lien' (sans routeur intermédiaire)
- **Obligatoire** pour la communications entre nœuds IPv6 (utilisé par les routeurs, découverte de voisins, pour la configuration d'adresses globales)
- Format: **FE80::/10**



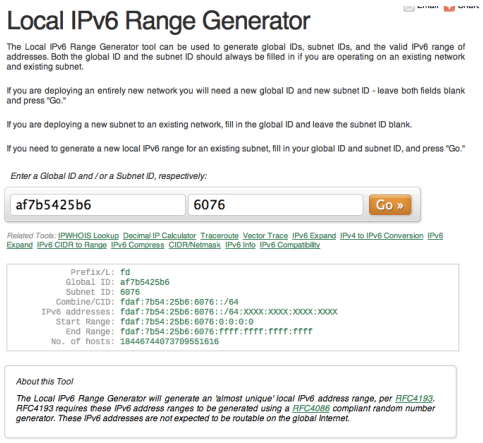
Adresses **Unique-local Unicast**

- Prévues pour être routées entre site via des tunnels (VPNs) ou à l'intérieur d'un site.
- **Préfixe**: FC00::/7, FC00::/8, FD00::/8
- **Non routable** sur Internet
- **Global ID**: Unique (choisi pseudo-aléatoirement, haute prob. d'unicité, RFC 4193)
- Bit L: positionné à 1 si le préfixe est fixé localement. 0: usage futur.
- Format:



UltraTools.com

- Pour générer des adresses aléatoirement, selon la RFC 4193:



Local IPv6 Range Generator

The Local IPv6 Range Generator tool can be used to generate global IDs, subnet IDs, and the valid IPv6 range of addresses. Both the global ID and the subnet ID should always be filled in if you are operating on an existing network and existing subnet.

If you are deploying an entirely new network you will need a new global ID and new subnet ID - leave both fields blank and press "Go."

If you are deploying a new subnet to an existing network, fill in the global ID and leave the subnet ID blank.

If you need to generate a new local IPv6 range for an existing subnet, fill in your global ID and subnet ID, and press "Go."

Enter a Global ID and / or a Subnet ID, respectively:

af7b5425b6 6076 Go »

Related Tools: IPWHOIS Lookup Decimal IP Calculator Traceroute Vector Trace IPv6 Expand IPv4 to IPv6 Conversion IPv6 Expand IPv6 CIDR to Range IPv6 Compress CIDR/Netmask IPv6 Info IPv6 Compatibility

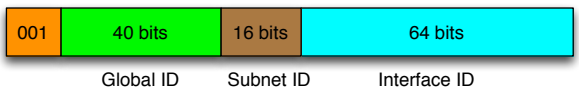
Prefix/L: fd
Global ID: af7b5425b6
Subnet ID: 6076
Combine/CID: fdaf:7b54:25b6:6076::/64
IPv6 addresses: fdaf:7b54:25b6:6076::/64:XXXX:XXXX:XXXX:XXXX
Start Range: fdaf:7b54:25b6:6076:0:0:0:0
End Range: fdaf:7b54:25b6:6076:ffff:ffff:ffff:ffff
No. of hosts: 18446744073709551616

About this Tool

The Local IPv6 Range Generator will generate an 'almost unique' local IPv6 address range, per RFC4193. RFC4193 requires these IPv6 address ranges to be generated using a RFC4086 compliant random number generator. These IPv6 addresses are not expected to be routable on the global Internet.

Adresses globales unicast avec agrégation

- Idée similaire à CIDR
  - L'Internet à une structure hiérarchique
    - Réseaux backbone, ISPs, clients
  - Le schéma doit permettre l'agrégation d'adresses à plusieurs niveaux afin de réduire la taille des tables de routage
- Structuration selon la RFC 3587
  - RFC 2374 (TLA, NLA): obsolète (dès 2003)
  - TLA/NLA remplacé par une politique d'allocation des RIRs.
  - Global ID: pour la topologie publique. Subnet ID: topologie du site



Quelques adresses globales unicast

- Bloc **2000::/3** (préfixe binaire: 001) réservé pour les adresses globales unicast routables sur Internet

Organisation	Adresses
Switch	2001:620::/32
HES-SO	2001:620:330::/48
HEIG-VD	**2001:620:540::/48**
EPFL	2001:620:618::/48
EPFZ	2001:620:8::/48
Swisscom	2a02:1200::/27
Teredo	2001::/32
6to4	2001:::/16

IPv6 à la HEIG-Vd (IICT)

```
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:00:F8:7A:24:86
          inet addr:10.192.74.56  Bcast:10.192.74.63  Mask:255.255.255.192
          inet6 addr: 2001:620:540:aaaa:200:f8ff:fe7a:2486/64 Scope:Global
          inet6 addr: fe80::200:f8ff:fe7a:2486/64 Scope:Link
          inet6 addr: 2001:620:540:aaaa::3/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:1 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:898 (898.0 B)  TX bytes:1684 (1.6 KiB)
          Interrupt:9 Base address:0xec00
```

Notion des masques de sous-réseau

- Ensemble d'adresses IPv6 commençant par la même séquence binaire
- Exemple: 2001:db8:1:1a0::/59 est le sous-réseau correspondant aux adresses comprises entre
  - 2001:db8:1:1a0:0:0:0:0 et
  - 2001:db8:1:1bf:ffff:ffff:ffff:ffff

Architecture des adresses

- Les adresses à usage local peuvent être réutilisées
  - Les adresses de site peuvent être réutilisées sur des sites d'une même organisation.
  - Zones dans lesquelles les nœuds sont attachés, adresses %zone ID
  - Zones ID: Interfaces (Link local pour Windows par exemple)
  - Exemple: fe80::1234 peut être représenté comme suit: fe80::1234%5 (sur le 5ème interface du nœud)

Adresses spécifiques
(RFC 4291 et 5156)

- Adresses de loopback
  - « 0:0:0:0:0:0:0:1/128 » ou « ::1/128 » en notation abrégée
  - Utilisée pour la communication inter-processus sur un nœud
  - Un peu comme 127.0.0.1 avec IPv4
- Adresse indéterminée
  - Composée uniquement de zéros
    - notation abrégée « ::/128 »
  - Utilisée pendant l'initialisation d'un nœud (initie une requête DHCP ou une Duplicate Address Detection, DAD)

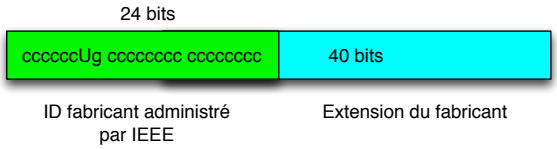
Source: Davies

IPv6 Interface Identifier

- Les 64 bits « Interface ID » (longueur fixe! Pas comme avec IPv4) d'une adresse unicast peuvent être assignés de diverses manières:
  - Autoconfiguré à partir d'une adresse MAC de 48 bits (comme Ethernet), étendue à 64 bits
  - Par DHCPv6 (stateful)
  - Autoconfiguré par un nombre aléatoire pour garantir l'anonymat (RFC 3041)

IPv6 Interface Identifier

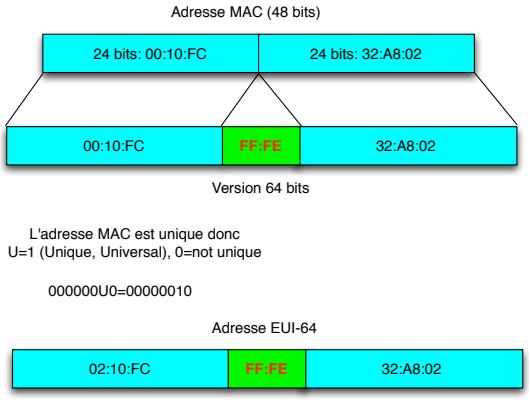
- Adresse EUI-64 (Extended Unique Identifier)



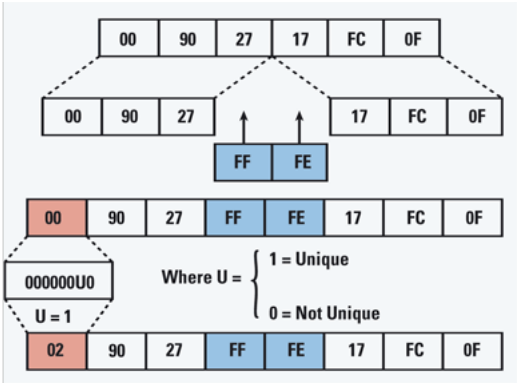
- U/L bit, U: 1 (Universally administrated) ou 0 (Locally administrated)

Interface ID (MAC -> EUI-64)

- Interface Id
  - Format défini par la norme IEEE EUI-64
  - Doit être unique au niveau global
  - Construction à partir d'une adresse MAC
    - Ajouter les octets FFFE entre les 3 premiers octets (fournisseur) et les 3 derniers octets (numéro de série de la carte)



Interface ID (MAC -> EUI-64)



http://www.zid.tuwien.ac.at/zidline/zl15/ipv6.html

ID des interfaces

- Cisco et Microsoft Windows (2003 et XP) utilisent le format EUI-64 comme vu précédemment
- Microsoft Windows 6 (Vista/2008) utilisent un identificateur aléatoire pour la « Link-Local Address »

```
Connection-specific DNS Suffix  . : localdomain
Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . . . . . : 00-0C-29-D0-C9-CF
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::91c8:133d:814f:70ff%11(Preferred)
```

– On peut désactiver ceci pour obtenir une adresse EUI-64

```
C:\Users\IICT>netsh interface ipv6 set global randomizeidentifiers=disabled
The requested operation requires elevation (Run as administrator).
```

Conversion d'une adresse MAC en EUI-64 (résumé)

- Adresse MAC d'un host: 00-0C-29-D0-C9-CF

1. Conversion en format EUI-64
   - 00-0C-29-FF-FE-D0-C9-CF
2. Complementer le bit U/L
   - Le premier octet est 0000 0000. Le septième bit doit être complémenté: 0000 0010 -> 02.
3. Conversion en notation hexadécimale
   - 20C:29FF:FED0:C9CF
4. Adresse de lien locale
   - FE80::20C:29FF:FED0:C9CF

ID d'adresses temporaires

- Aujourd'hui: adresses IPv4 distribuées via un ISP avec PPP-> adresses différentes en général.
- Adresse IPv6 globale: comprend la partie EUI-64 -> l'utilisateur peut être identifié (et peut être suivi par des vendeurs, personnes mal intentionnées,…)
- Alternative: offrir le même niveau d'anonymat qu'avec IPv4 (RFC 3041): génération aléatoire de l'ID de l'interface.
  - Implémenté par Windows (pas sur les routeurs)

ID adresses temporaires (2)

- ID initial de l'interface: généré aléatoirement.
  - Duplicate Address Detection (DAD) nécessaire
- Principe du choix de l'ID de l'interface (RFC 3041):
  1. Prendre la valeur de l'itération précédente de l'algorithme (ou une valeur aléatoire s'il n'y en a pas)
  2. Calculer le MD5 de la valeur mémorisée précédemment -> hash de 128 bits
  3. Prendre les 64 bits de gauche et mettre le sixième bit à 0 (bit U/L). Ceci va créer l'identificateur de l'interface. Garder cette valeur
  4. Prendre les 64 bits de droite et les garder pour la prochaine itération de l'algorithme

ID adresses temporaires (3)

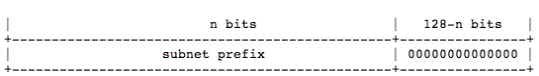
- Choix de MD5: bonnes propriétés de randomization!
  - En l'absence de mémorisation: génération pseudo-aléatoire chaque fois
- Changement temporaire de l'identificateur de l'interface lorsque le timer expire.
  - Valeurs annoncées par le routeur. Avec Windows, le temps de renouvellement standard est de 1 jour/ 1 semaine.

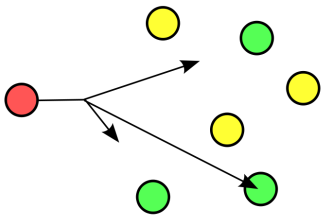
Type d'adresses

- Adresses anycast
  - Adresse d'un ensemble d'interfaces. Le paquet est en général traité par l'interface le plus proche.
- Adresses multicast
  - Adresse d'un ensemble d'interfaces. Les paquets sont traités par tous les interfaces.

Type d'adresses

- Adresses anycast
  - Adresse d'un ensemble d'interfaces. Le paquet est en général traité par l'interface le plus proche.
  - Ce ne sont que les routeurs qui vont répondre aux adresses anycast
  - Sont prises dans l'espace d'adressage des adresses unicast
  - Format (RFC 4291)

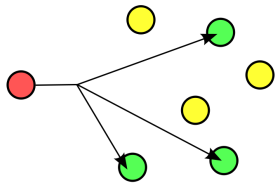




Wikipedia

Type d'adresses

- Adresses multicast
  - Identifie un groupe d'interfaces ou de nœuds
  - Ne peuvent pas être utilisées commes adresses de source
  - Un interface doit appartenir à un groupe



Wikipedia

Type d'adresses

- Adresses **multicast**
  - Adresse d'un ensemble d'interfaces. Le paquet est en général traité par l'interface le plus proche
  - Format (RFC 4291): **FF00::/8**

  - Flags: ORPT (RFC 3956, RFC3306)
    - T: Transitoire ou bien connue (IANIA)
  - Scop (4 bits): Limite la portée de la propagation multicast (interface, Link, Site, Glabal, Organisation)

Adresses multicast bien connues

Address(s)	Description	Reference
FF01:0:0:0:0:0:0:1	All Nodes Address	[RFC4291]
FF01:0:0:0:0:0:0:2	All Routers Address	[RFC4291]
FF01:0:0:0:0:0:0:FB	mDNSv6	[RFC-cheshire-dnsext-multicastdns-15]

Address(s)	Description	Reference
FF02:0:0:0:0:0:0:1	All Nodes Address	[RFC4291]
FF02:0:0:0:0:0:0:2	All Routers Address	[RFC4291]
FF02:0:0:0:0:0:0:3	Unassigned	[Jon_Postel]
FF02:0:0:0:0:0:0:4	DVMRP Routers	[RFC1075][Jon_Postel]
FF02:0:0:0:0:0:0:5	OSPFIGP	[RFC2328][John_Moy]
FF02:0:0:0:0:0:0:6	OSPFIGP Designated Routers	[RFC2328][John_Moy]
FF02:0:0:0:0:0:0:7	ST Routers	[RFC1190][<mystery contact>]
FF02:0:0:0:0:0:0:8	ST Hosts	[RFC1190][<mystery contact>]
FF02:0:0:0:0:0:0:9	RIP Routers	[RFC2080]

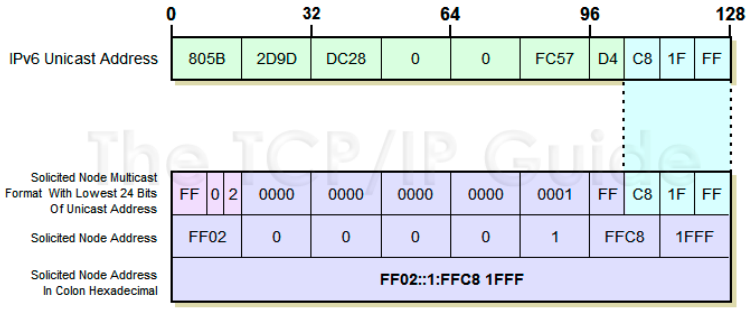
Address(s)	Description	Reference
FF05:0:0:0:0:0:0:2	All Routers Address	[RFC4291]
FF05:0:0:0:0:0:0:FB	mDNSv6	[RFC-cheshire-dnsext-multicastdns-15]
FF05:0:0:0:0:0:1:3	All-dhcp-servers	[RFC3315]

http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml

Sollicitated-node multicast

- Pour chaque adresse unicast et anycast il existe une adresse « sollicitated-node multicast » correspondante (qui évite d'utiliser l'adresse « all-node multicast »)
- Usage
  - Neighbour sollicitation messages
  - Duplicated address detection message (DAD)
- Format
  - **FF02::1:FF-last 24 bits**

Sollicitated-node multicast



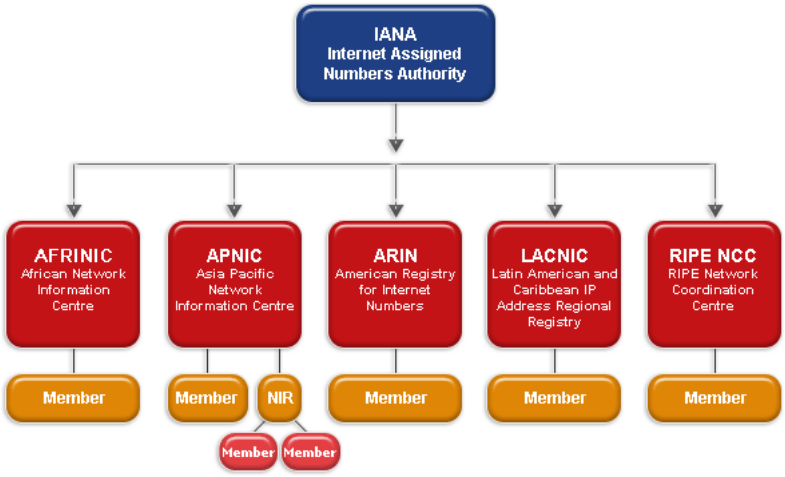
Tcpip guide

IANA (Internet Assigned NumbersAuthority)

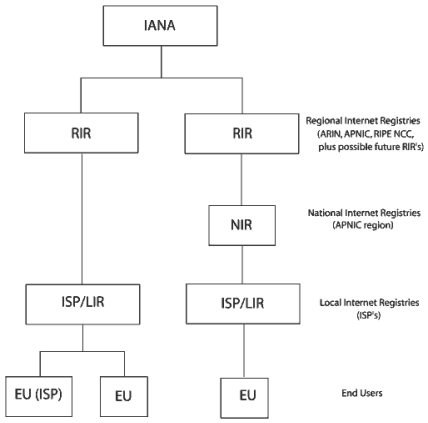
Registry	Area Covered
AfriNIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

- Adresses individuelles: viennent d'un ISP
- Les ISP obtiennent les plages d'adresses IP des Local Internet Registry (LIR) ou des National Internet Registry (NIR) ou des Regional Internet Registry (**RIR**)

Allocation des préfixes IPv6, hiérarchie



Allocation des préfixes IPv6, hiérarchie



http://www.ripe.net/ripe/docs/ripe-552

Exemple d'allocation d'adresses IPv6 globales

- Adresse unicast
  - 2000::/3 Global Unicast IANA complete pool
  - 2001::/16 Global Unicast IANA allocated pool
  - 2001:800::/23 RIPE NCC
  - 2001:918::/32 Swissom IP-Plus Internet Services (ISP)
    - 2001:918:fff8::/48 LANexpert SA
  - 2001:620::/32 Switch
    - **2001:620:540::/48 HEIG-Vd**
    - 2001:620:618::/48 EPFL
    - 2001:620:8::/48 ETH

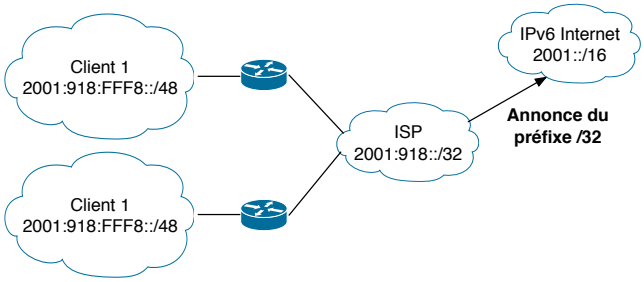
Fournisseur principaux en Suisse

Top 25 internet service providers for IPv6 in Switzerland (Dec 2012)

	ISP	IPv6 tests count
1.	Hurricane Electric	325
2.	Init Seven AG	169
3.	Swisscom 6RD	145
4.	Switch	119
5.	Swisscom IP-Plus TLA	115
6.	IP-Max assigned	39
7.	cablecom GmbH	32
8.	Sunrise	24
9.	RIPE Network Coordination Centre	19
10.	gogo6 Inc.	14
11.	Cern	14
12.	Dolphins	13
13.	Monzoon	13
14.	As8758	11
15.	Achermann ict-services AG	11
16.	Swisscom (Schweiz) AG - Bluewin	9
17.	Nine Internet Solutions AG	5

http://ipv6-test.com/stats/country/CH

Adressage hiérarchique et aggrégation



- Les adresses IPv6 sont aggrégeables avec des préfixes de longueur arbitraire (comme avec CIDR)
- Avantages de l'aggrégation:
  - Réduction de la dimension des tables de routage
  - Utilisation possible d'un préfixe global différent

Nouvelle fonctionnalité : Découverte de voisins

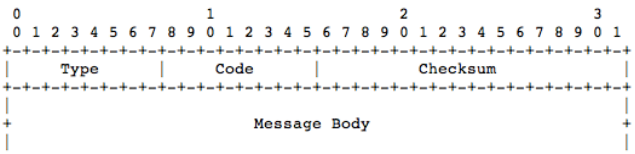
- *Neighbor discovery* (RFC 2461)
- Remplace le protocole ARP
- Implémentée à l'aide de nouveaux messages ICMPv6
  - Message 'Sollicitation de voisins' (neighbor sollicitation)
    - Envoyé à l'adresse multicast 'All nodes' du 'lien'
    - Contient l'adresse IPv6 du nœud cherché
  - Message 'Annonce d'un voisin'
    - Envoyé en réponse à une sollicitation ou spontanément
    - Contient l'adresse IPv6 et physique (MAC) du nœud

ICMPv6 (RFC 4443)

- Version mise à jour de ICMP (Internet Control Message Protocol) pour IPv6
- Signale les erreurs liés à l'acheminement des paquets + service d'écho (ping)
- Fourni un cadre pour:
  - Multicast Listener Discovery (MLD): correspond à IGMP (rappel: protocole entre hosts et routeurs adjascents, multicast) avec IPv4
  - Neighbor Discovery (ND): remplace ARP, ICMP Router Discovery et ICMP Message Redirect en IPv4
  - Secure Neigbor Discovery (SEND): pas supporté par Windows (8, Server 2012, Vista, …)
  - Mobilité IPv6

ICMPv6

- Format:



  - Type:
    - 1: Destination Unreachable
    - 2: Packet Too Big
    - 3: Time Exceeded
    - 4: Parameter Problem
    - 128: Echo Request
    - 129: Echo Reply
  - Messages d'erreur: type 0-127.
  - Messages informels: type 128-255

ICMPv6

- Code (exemple)

Type 1 - Destination Unreachable

Reference
[RFC4443]

Code	Name	Reference
0	no route to destination	
1	communication with destination administratively prohibited	
2	beyond scope of source address	[RFC4443]
3	address unreachable	
4	port unreachable	
5	source address failed ingress/egress policy	[RFC4443]
6	reject route to destination	[RFC4443]
7	Error in Source Routing Header	[RFC6550][RFC6554]

www.iana.org

- Checksum: calculé sur le message ICMPv6 entier + pseudo entête IPv6

Comparaison des messages ICMPv4 et ICMPv6

Common ICMPv4 Message	ICMPv6 Equivalent
Destination Unreachable- Network unreachable (Type 3, Code 0)	Destination Unreachable-No route to destination (Type 1, Code 0)
Destination Unreachable-Protocol unreachable (Type 3, Code 2)	Parameter Problem-Unrecognized Next Header field (Type 4, Code 1)
Destination Unreachable-Port unreachable (Type 3, Code 3)	Destination Unreachable-Port unreachable (Type 1, Code 4)
Destination Unreachable-Fragmentation needed and DF set (Type 3, Code 4)	Packet Too Big (Type 2, Code 0)
Time Exceeded-TTL expired (Type 11, Code 0)	Time Exceeded-Hop Limit exceeded (Type 3, Code 0)
Parameter Problem (Type 12, Code 0)	Parameter Problem (Type 4, Code 0 or 2)
Redirect (Type 5, Code 0)	Neighbor Discovery Redirect message (Type 137, Code 0).

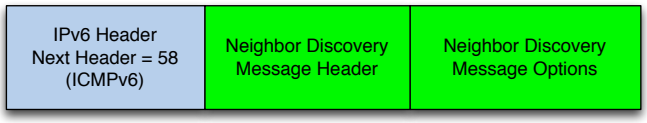
Joseph Davies, Understanding IPv6

Quiz

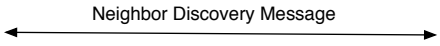
- Comment distinguer les messages ICMPv6 d'erreur et les messages informels?

Network Discovery Protocol (NDP)

- Format:



- Rappel



  - ND remplace ARP, ICMPv4 Router Discovery et ICMPv4 Message Redirect
- Nouveaux messages:
  - Router sollicitation (ICMPv6, type 133)
  - Router Advertisement (ICMPv6, type 134)
  - Neighbor Sollicitation (ICMPv6, type 135)
  - Neighbor Advertisement (ICMPv6, type 136)
  - Redirect (ICMPv6, type 137)

Network Discovery Protocol (NDP)

- ND utilisé par les nœuds
  - Pour trouver les routeurs voisins
  - Autoconfigurer des adresses, des préfixes d'adresses et d'autres paramètres de configuration
- ND est utilisé par les routeurs
  - Pour signaler leur présence, donner des préfixes, configurer des hôtes
  - Informer les hôtes sur de meilleures adresses (next hop) pour forwarder des paquets vers une destination spécifique
- Messages ICMPv6: types 133 à 137
- Les messages ND restent dans le réseau local -> hop limit à 255

Options de ND

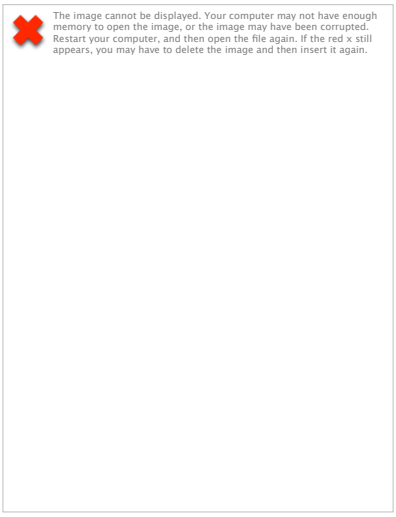
- Option de ND: Type sur 8 bits en format TLV (Type-length-value)
  - Type 1: Source Link-Layer Address
    - Compléter p. 134 Davies
  - Type 2: Target Link-Layer Address
  - **Type 3: Prefix Information**
  - Type 4: Redirected Header
  - Type 5: MTU
  - Type 7: Advertisement Interval
  - Type 8: Home Agent Information
  - Type 24: Route Information

Durée de vie de l'adresse (lifetime)

- Option de type 3 (Prefix Information)
  - Valid Lifetime: Nombre de secondes de validité de l'adresse basée sur le préfixe donné. Codé su r32 bits. 0xFFFFFFFF signifie « infini ».
  - Preferred Lifetime: Nombre de secondes pendant lesquelles l'adresse reste dans un état « préféré ». Ensuite l'adresse rentre dans un état « déprécié » (qui peut être valide)

Router Sollicitation/Advertisement

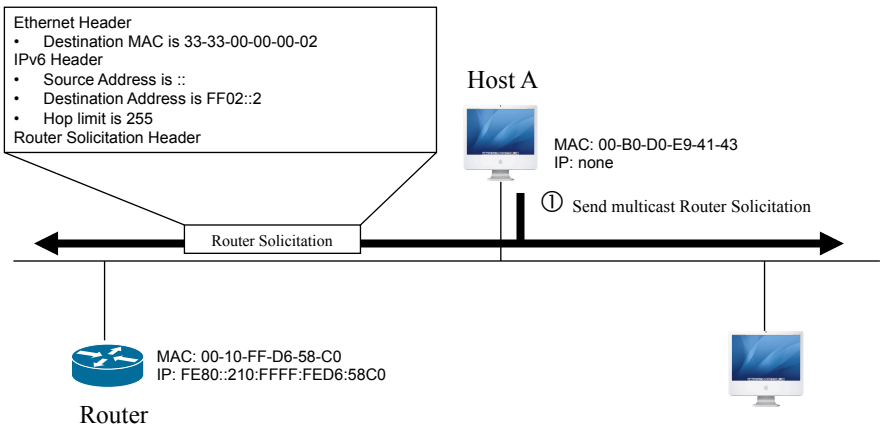
- **Router Sollicitations:** envoyées surtout par des nœuds qui arrivent sur le réseau (ou reconfigurartion de leurs interfaces, ifconfig/ renew6)
- **Les routeurs envoient régulièrement** des Router Advertisements sur le réseau (all-nodes multicast)



Router Sollicitation

- Les hôtes envoient ce message pour avoir une réponse immédiate au lieu de devoir atttendre le message d'un routeur (Router Advertisement)
  - Adresse MAC source: adresse MAC de l'interface
  - Adresse MAC de destination: 33-33-00-00-00-02
  - Adresse IPv6 de source: link-local ou non spécifiée (::)
  - Adresse IPv6 de destination: FF02::2 (all-router multicast)
  - Hop limit: 255
  - ICMPv6 Type: 133
  - Code: 0
  - Checksum

Router Sollicitation (multicast message)



Joseph Davies, Understanding IPv6

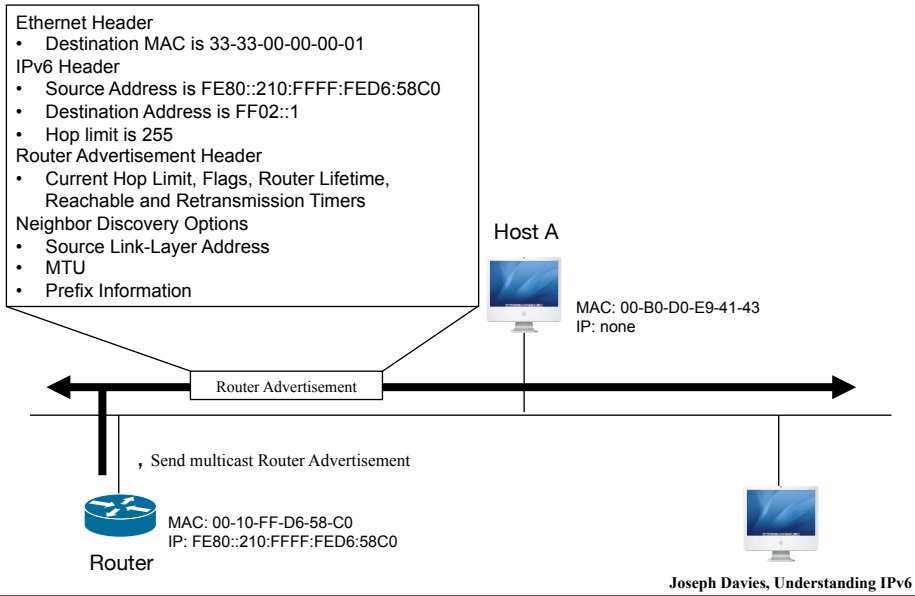
Router Advertisement

- Les messages non sollicités sont envoyés à intervalles pseudo-aléatoires
- Les messages sollicités sont des réponses à des sollicitations d'hôtes
  - Adresse MAC source: adresse MAC de l'interface
  - Adresse MAC de destination: 33-33-00-00-00-01 (ou adresse MAC unicast du host qui a envoyé la sollicitation)
  - Adresse IPv6 de source: «link-local address» assignée à l'interface de la source
  - Adresse IPv6 de destination: FF02::1 (all-router multicast)
  - Hop limit: 255
  - ICMPv6 Type: 134
  - Code: 0
  - Checksum

Router Advertisement

- Current Hop limit
- Managed Address Configuration flag
- Other Stateful Configuration flag
- Home Agent flag
- Default Router Preference
- Reserved
- Router Lifetime
- Reachable Time
- Retransmission Timer
- Options (MTU, Advertisement Interval, Route,…)

Router Advertisement (multicast message)



Joseph Davies, Understanding IPv6

Capture (HEIG-Vd)

```
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x9bb3 (correct)
    Cur hop limit: 64
    Flags: 0x00
        0... .... = Not managed
        .0.. .... = Not other
        ..0. .... = Not Home Agent
        ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans time: 0
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:03:e3:bb:f1:b2
    ICMPv6 options
        Type: 5 (MTU)
        Length: 8 bytes (1)
        MTU: 1500
    ICMPv6 options
        Type: 3 (Prefix information)
        Length: 32 bytes (4)
        Prefix length: 64
        Flags: 0xc0
            1... .... = Onlink
            .1.. .... = Auto
            ..0. .... = Not router address
            ...0 .... = Not site prefix
        Valid lifetime: 0x00278d00
        Preferred lifetime: 0x00093a80
        Prefix: 2001:620:540:aaaa::
```

Neighbor Sollicitation

- Les nœuds IPv6 envoient un message NS pour trouver l'adresse de lien (link-layer) d'un nœud ou pour confirmer une adresse de lien existante en cache
- Exemple: Ethernet
  - Adresse MAC de source: adresse MAC de l'interface de la source
  - Adresse MAC de destination: 33-33-FF-XX-XX-XX (derniers 24 bits du nœud sollicité)
  - Adresse IPv6 de source: link-local ou non spécifié (::)
  - Adresse IPv6 de destination: FF02::FFXX:XXXX (nœud sollicité en multicast)
  - Hop Limit field: 255, ICMPv6 Type: 133, Code: 0, Checksum, Reserved, Target Address + options

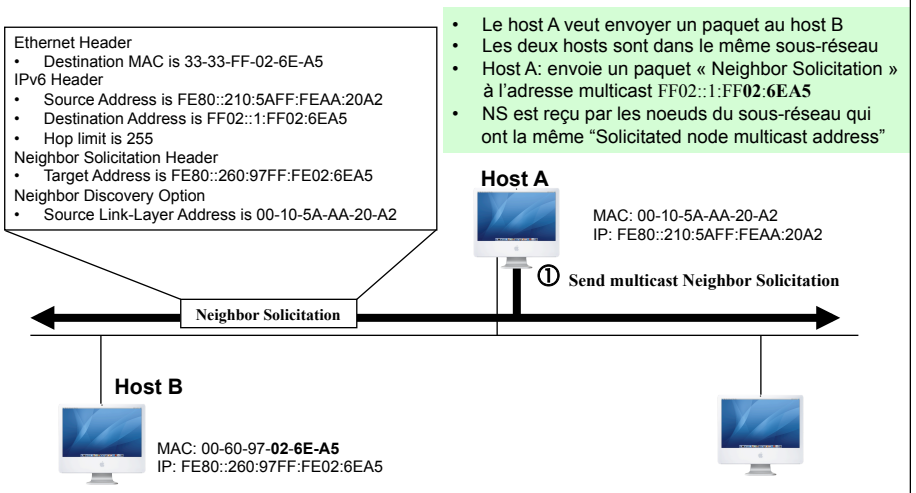
Neighbor Advertisement

- Utilisé par les nœuds pour répondre à un « Neighbor Sollicitation »
- Un nœud IPv6 peut aussi envoyer un message pour informer son voisionnage d'un changement (rôle du nœud ou changement d'adresse de lien)
- Exemple
  - Adresse de source MAC: adresse MAC de l'interface source
  - Adresse de destination MAC: adresse MAC du nœud auquel on répond
  - Adresse IPv6 source: adresse unicast de la source
  - Adresse IPv6 destination: adresse unicast du nœud auquel on répond

Neighbor Advertisement

- Exemple (suite)
  - Hop Limit field: 255
  - Type: 136
  - Code: 0
  - Checksum
  - Router flag (0: node; 1: router)
  - Solicited flag
  - Override flag
  - Reserved
  - Target Address
  - Options
- Quand le message n'est pas sollicité
  - Adresse MAC de destination: 33-33-00-00-00-01 (all-nodes)
  - Adresse IPv6 de destination: FF02::1 (all-nodes muilticast)

Résolution d'adresses avec IPv6: Network Discovery Protocol (NDP)

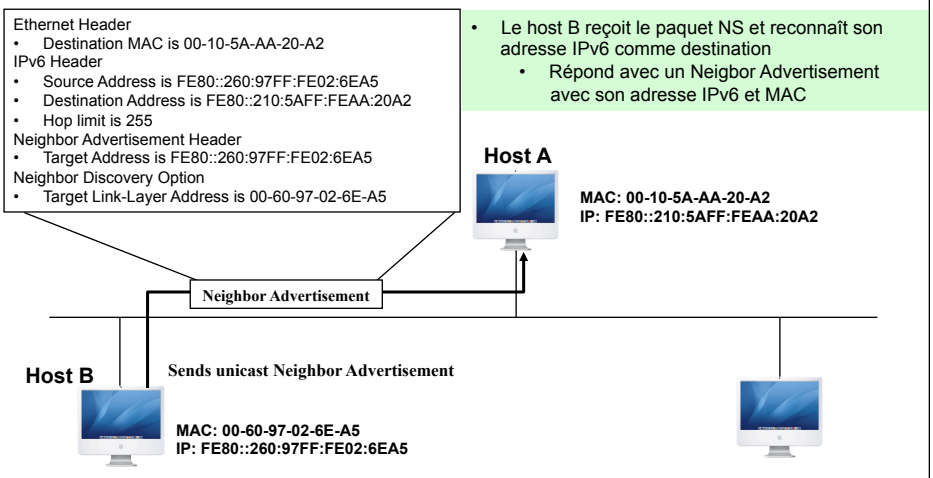


Joseph Davies, Understanding IPv6

Rappel: Sollicitated-node multicast

- Pour chaque adresse unicast et anycast il existe une adresse « sollicitated-node multicast » correspondante (qui évite d'utiliser l'adresse « all-node multicast »)
- Un paquet avec une telle adresse de destination est forwardé par le niveau 2 à tous les nœuds qui écoutent cette adresse multicast
- Mieux que de faire une diffusion
- Format
  - **FF02::1:FF-last 24 bits**

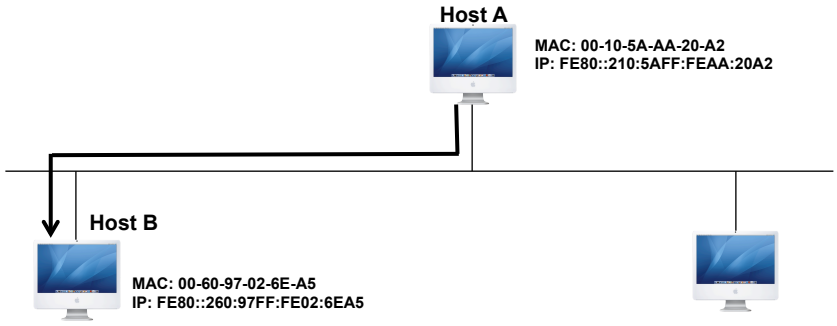
Résolution d'adresses avec IPv6: Network Discovery Protocol (NDP)



Joseph Davies, Understanding IPv6

Résolution d'adresses avec IPv6: Network Discovery Protocol (NDP)

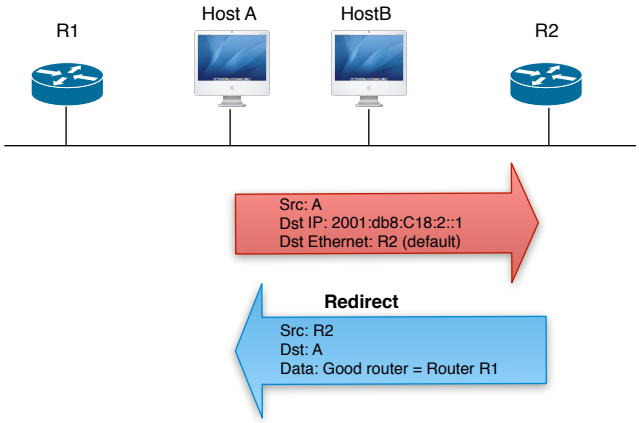
- Le host A lit le NA et garde les informations dans son cache
- Envoie des paquets à Host B (trafic unicast)
- Le cache expire si aucun trafic n'est envoyé (cache timeout)



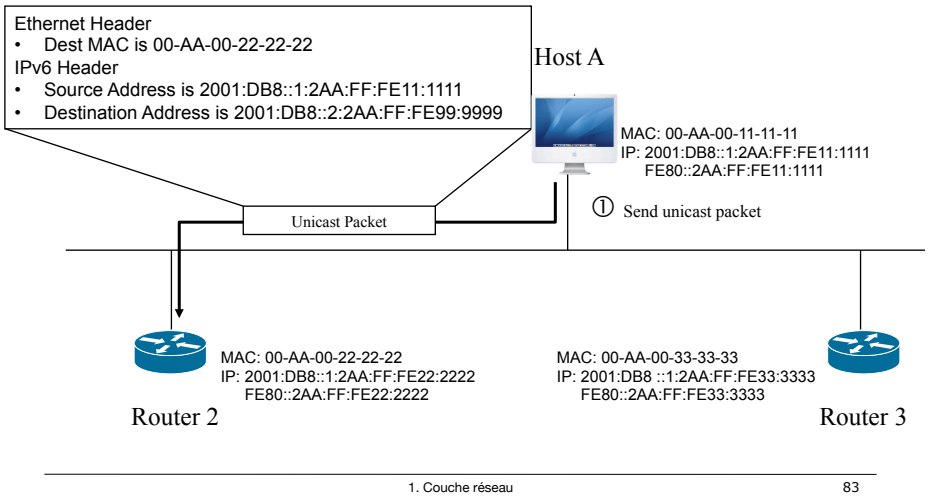
Joseph Davies, Understanding IPv6

Redirect

- Le message « redirect » informe la source qu'il existe un meilleur routeur pour le premier pas.

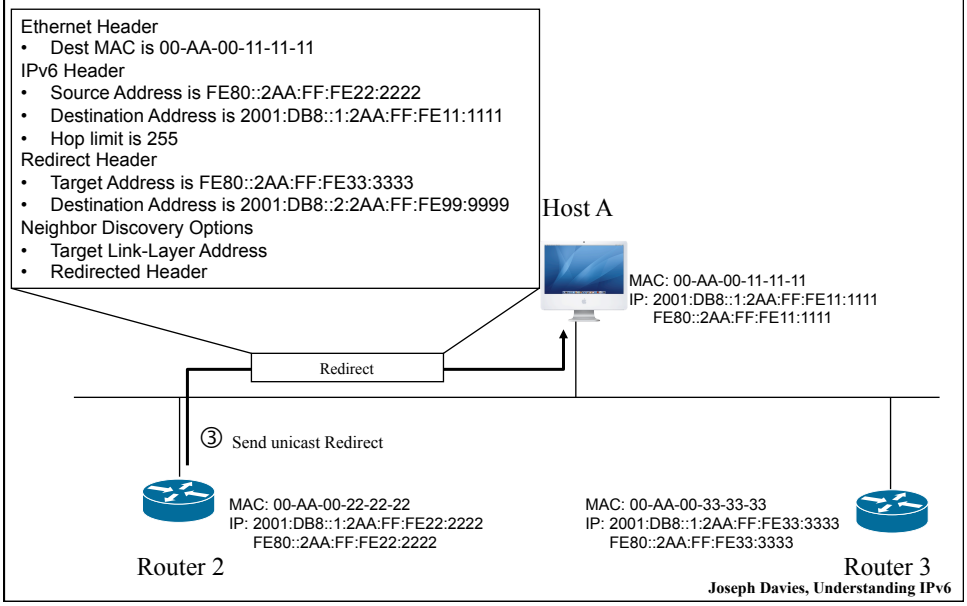


Paquet unicast vers le routeur



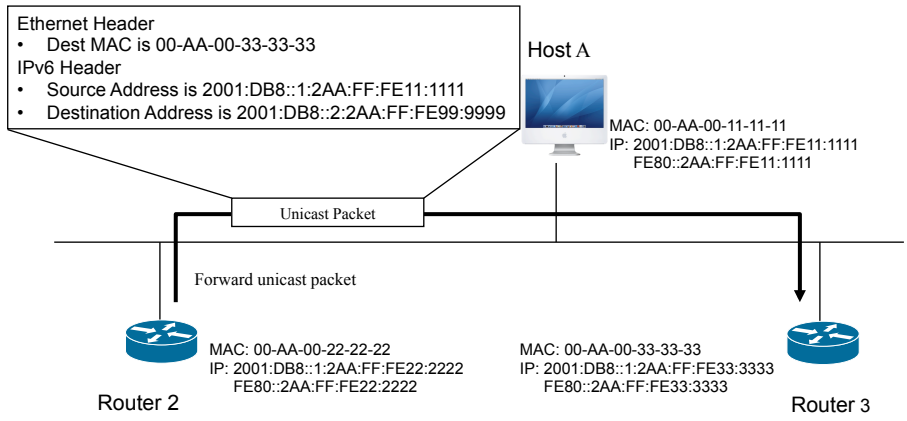
Joseph Davies, Understanding IPv6

Paquet de redirection envoyé par le routeur



Joseph Davies, Understanding IPv6

Paquet unicast envoyé par le routeur

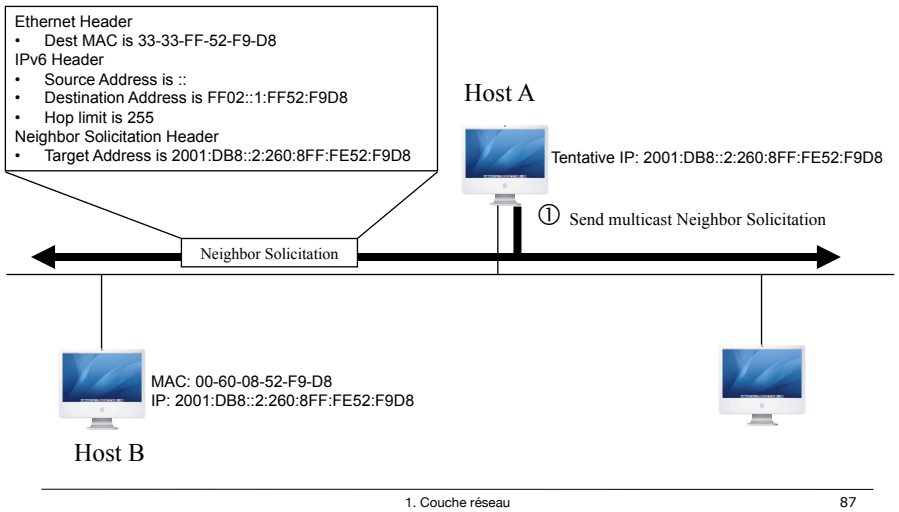


Joseph Davies, Understanding IPv6

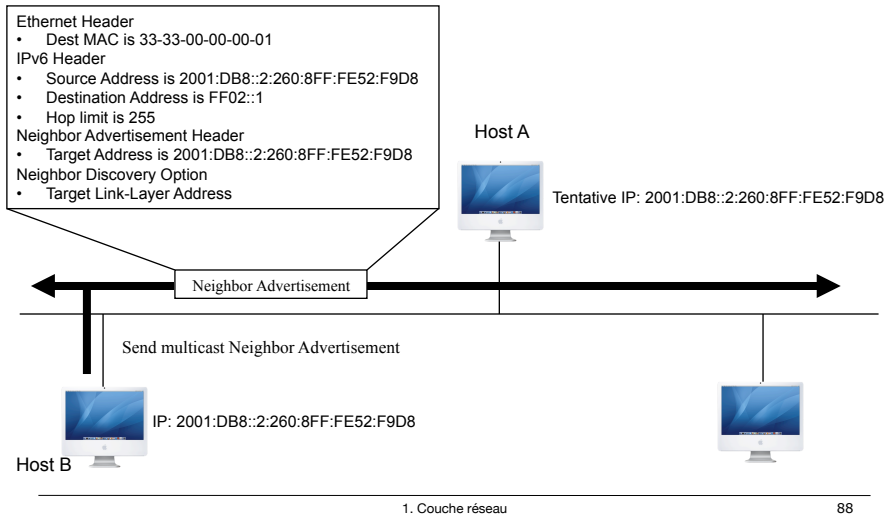
Duplicate Address Detection (DAD)

- IPv4: Utilisation de ARP (gratuitous ARP) pour détecter des doublons d'adresses dans le sous-réseau
- IPv6: Neighbor Sollicitation (RFC 4862)
  - L'adresse concernée se trouve dans le champ « Target Address » de la sollicitation
  - Adresse de source: non spécifiée (::)
- S'il y a doublon d'adresse, le nœud envoie un « Neighbor advertisement » en multicast
  - Adresse de destination: all-node multicast (FF02::1)

Duplicate Address Detection (DAD)



Duplicate Address Detection (DAD)



Configuration automatique sans état (résumé)

- Facilité la gestion du réseau des stations terminales, non pas des routeurs
- Basée sur les 2 nouveaux messages ICMPv6
  - Message ICMPv6 'Sollicitation des routeurs'
  - Message ICMPv6 'Annonce d'un routeur'
    - Envoyé périodiquement ou après une sollicitation
      - Inclut des options pour signaler la MTU du lien, …
      - Indique si l'auto-configuration sans état est permise et le préfix du sous-réseau à utiliser
      - Peut limiter la durée de vie du préfixe indiqué
- Algorithme
  1. La station construit une adresse locale de lien
     - Préfix 'FE80::' plus l'ID de l'interface (--> MAC)
     - Le nœud teste s'il y a un conflit en envoyant un message 'Sollicitation de voisins'
  2. La station envoie une sollicitation de routeurs à l'adresse multicast 'All routers' du lien
  3. Le routeur renvoie une annonce de routeur avec un préfixe du sous-réseau
  4. La station obtient une adresse globale en concaténant le préfixe avec l'ID de l'interface

Configuration automatique avec état

- Basée sur l'utilisation d'un serveur DHCPv6
- Permet une meilleure contrôle de l'utilisation d'adresses

Configuration des hôtes

- IPv4:
  - Manuellement (adresse IP, masque, passerelle de défault, DNS)
  - Automatiquement: DHCPv4
- IPv6
  - Stateless Address Autoconfiguration (SLAAC): plug&play, unique avec IPv6, automatique
    - Réception des annonces des routeurs (information sur le préfixe, options)
  - DHCPv6 stateful
    - Serveur DHCP
  - Stateless et stateful

SLAAC

- But: éviter les serveurs DHCP
- Fonctionnement
  - Les hôtes configurent leurs adresses de lien (link-local)
  - Les préfixes sont obtenues via les annnonces des routeurs
- Ne fonctionne que pour IPv6 (pas IPv4)

Processus d'autoconfiguration (RFC 4862)

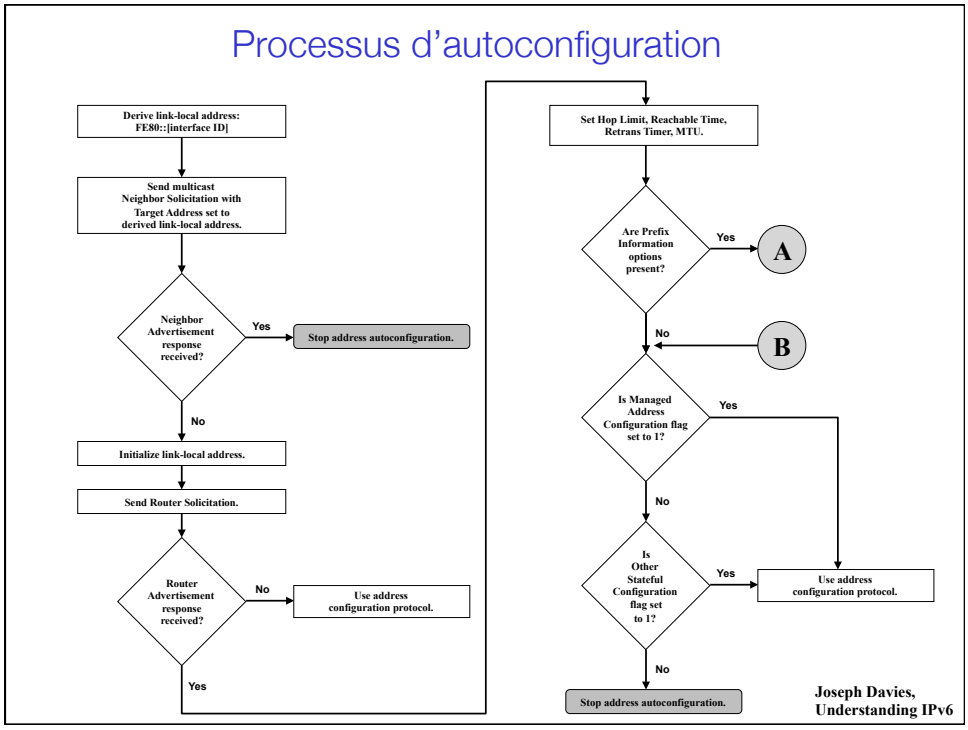
① Configuration de l'adresse locale de lien (link-local), basée
- Adresse MAC (EUI-64) + le préfixe FE80::/64
- Assignée aléatoirement
- Générée manuellement
- Adresse générée avec un algorithme cryptographique

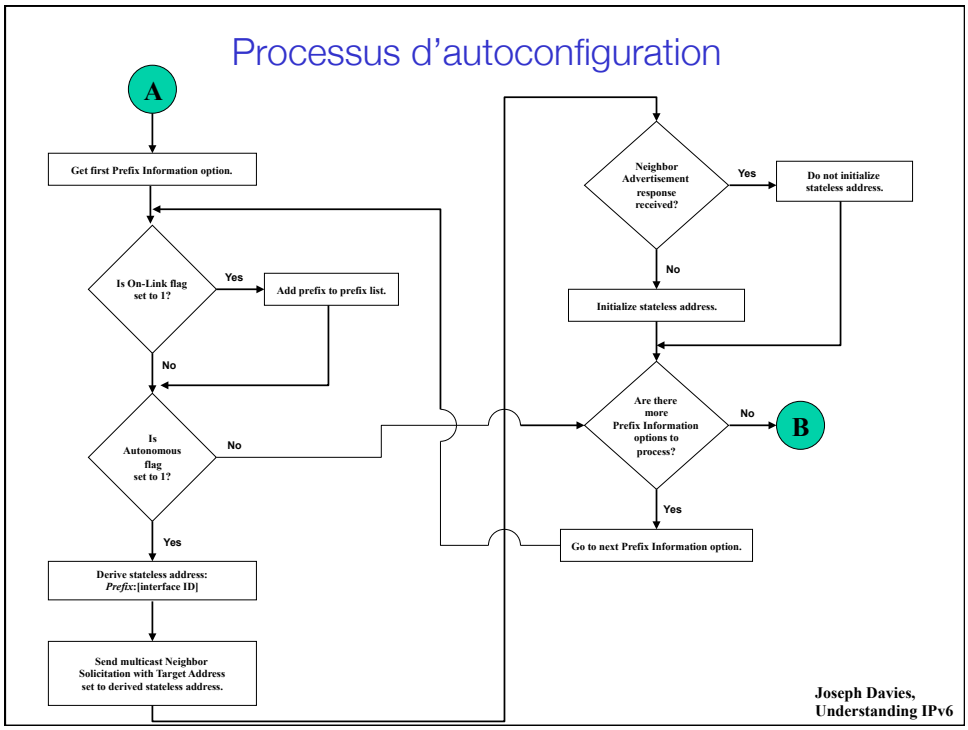
② Test d'unicité de l'adresse sur le lien local (Duplicate Address Detection)
- Si une annonce de voisin est reçue alors il y a un autre nœud qui utilise l'adresse locale. L'autoconfiguration est stoppée et une configuration manuelle doit être envisagée
- Si aucune annonce de voisin n'est reçue alors l'adresse locale est supposée unique. L'adresse multicast « sollicitated node address » est crée et enregistrée dans l'interface

Processus d'autoconfiguration (2)

③ Envoi d'une sollicitation au routeur
- Si aucune réponse n'est reçue alors l'hôte utilise l'adresse d'un protocole de configuration pour obtenir une adresse et les paramètres de configuration
- Si une réponse est reçue alors les paramètres suivants vont être retenus: Hop Limit, Reachable Time, Retransmission Timer, MTU

④ Si les informations sur le préfixe sont présentes:
- Les drapeaux «On-Link», «Autonomous» sont mis à 1
- Détection d'adresse dupliquée (DAD)
- Setting des paramètres: valid lifetime, prefered lifetime, ,…


Processus d'autoconfiguration
Derive link-local address: FE80::[interface ID]
Send multicast Neighbor Solicitation with Target Address set to derived link-local address.
Neighbor Advertisement response received?
Yes
Stop address autoconfiguration.
No
Initialize link-local address.
Send Router Solicitation.
Router Advertisement response received?
No
Use address configuration protocol.
Yes
Set Hop Limit, Reachable Time, Retrans Timer, MTU.
Are Prefix Information options present?
Yes
A
No
B
Is Managed Address Configuration flag set to 1?
Yes
No
Is Other Stateful Configuration flag set to 1?
Yes
Use address configuration protocol.
No
Stop address autoconfiguration.
Joseph Davies, Understanding IPv6


Processus d'autoconfiguration
A
Get first Prefix Information option.
Is On-Link flag set to 1?
Yes
Add prefix to prefix list.
No
Is Autonomous flag set to 1?
No
Yes
Derive stateless address: Prefix:[interface ID]
Send multicast Neighbor Solicitation with Target Address set to derived stateless address.
Neighbor Advertisement response received?
Yes
Do not initialize stateless address.
No
Initialize stateless address.
Are there more Prefix Information options to process?
No
B
Yes
Go to next Prefix Information option.
Joseph Davies, Understanding IPv6

Stateless DHCPv6 (RFC 3736)

- But: Résoudre les problèmes liés à l'autoconfiguration
  - Par exemple: l'adresse d'un serveur DNS n'est pas fournie à l'hôte pendant le processus d'autoconfiguration
- Comment est-ce que ça fonctionne?
  - L'autoconfiguration stateless est effectuée en premier
  - La réponse du routeur contient un drapeau = USE STATELESS DHCP
  - L'hôte envoie une requête au serveur DHCP pour obtenir les informations dont il a besoin (adresse d'un DNS par exemple)
- Pourquoi est-il appelé « stateless »?
  - Car il ne garde aucune information en mémoire (adresses ou autres)

DHCP (Rappel)

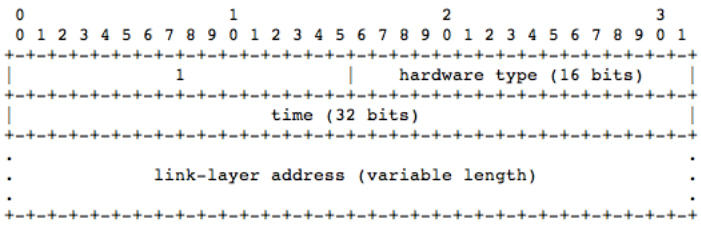
- But: éviter la configuration manuelle
- Comment est-ce que ça fonctionne?
  - Mettre les informations dans les serveurs
  - Les hôtes contactent le serveur lorsqu'ils arrivent sur le réseau (ou lors d'un «boot»)
  - Temps limités de réservation

Stateful DHCPv6

- Il n'y a plus de messages de diffusions
  - Les clients communiquent avec les serveurs DHCP en utilisant des adresses multicast FF02::1:2, All_DHCP_Relay_Agents_and_Servers et FF05::1:3 (All_DHCP_Servers) ou des adresses unicast.
  - Les hôtes utilisent leurs adresses locales et font un DAD avant de communiquer avec le serveur DHCP
  - DUID=DHCP Unique Identifier: Les clients/serveurs doivent en avoir un pour être identifiés
- Messages UDP
  - Les clients DHCPv6 écoutent le port UDP 546
  - Les serveurs et relais DHCPv6 écoutent le port UDP 547

DUID-LLT (RFC 3315)

DHCP Unique Identifier

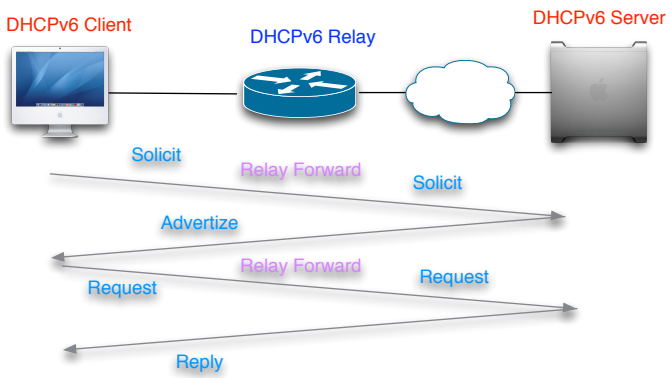


- Time: Temps auquel DUID a été généré en secondes depuis le 1 janvier 2000, modulo 2^{24}
- Hardware Type: type de hardware valid, selon la RFC 826
- Link-layer address: adresse valide (selon RFC 2464) d'un interface réseau connecté au dispositif DHCP quand le DUID est généré
- Autres DUID: basés sur des numéros assignés par l'entreprise (DUID-EN) ou seulement sur l'adresse (DUID-LL)

Echanges de messages avec Stateful DHCPv6

1. A Solicit message sent by the client to locate the servers.
2. An Advertise message sent by a server to indicate that it can provide addresses and configuration settings.
3. A Request message sent by the client to request addresses and configuration settings from a specific server.
4. A Reply message sent by the requested server that contains addresses and configuration settings.

DHCPv6

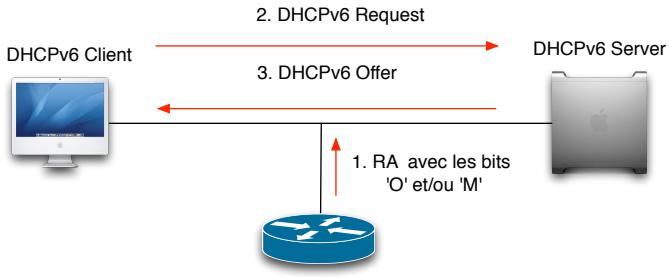


DHCPv6

- Fourni un service stateful ou stateless (basé sur la base des annonces des routeurs, Router Advertisements)
  - Managed Address Configuration (M) flag
  - Other Stateful Configuration (O) flag
- M=0, O=0
  - Réseau sans infrastructure DHCPv6
- M=1, O=1
  - DHCPv6 fourni les adresses et les autres paramètres de configuration
- M=0, O=1
  - DHCPv6 ne fourni que les autres paramètres de configuration
- M=1, O=0
  - DHCPv6 fourni les adresses uniquement

DHCPv6

- Le client DHCPv6 détecte la présence d'un routeur sur la ligne
- Le client examine le RA pour déterminer si DHCP peut être utilisé
- Si aucun routeur n'est trouvé
  - Envoi d'un message « sollicit » à l'adresse multicast All-DHCP-Agents
  - Utilisation de l'adresse de lien locale comme adresse de source



Pour info: Messages DHCP (en anglais)

- Solicit (equivalent à DHCP Discover)
  - Sent by a client to locate servers
- Advertise (DHCP Offer)
  - Sent by a server in response to a Solicit message to indicate availability
- Request (DHCP Request)
  - Sent by a client to request addresses or configuration settings from a specific server
- Confirm (DHCP Request)
  - Sent by a client to all servers to determine if a client's configuration is valid for the connected link
- Renew (DHCP Request)
  - Sent by a client to a specific server to extend the lifetimes of assigned addresses and obtain updated configuration settings

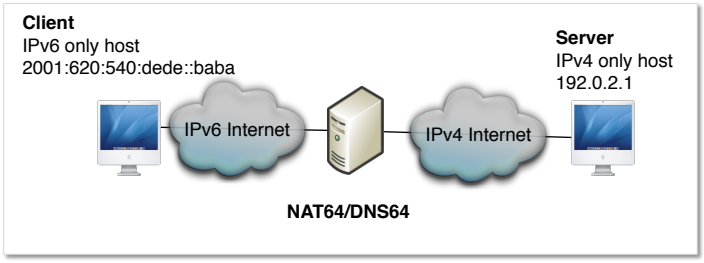
Pour info: Messages DHCP (en anglais)

- Rebind (DHCP Request)
  - Sent by a client to any server when a response to the Renew message is not received
- Reply DHCP Ack)
  - Sent by a server to a specific client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message
- Release (DHCP Release)
  - Sent by a client to indicate that the client is no longer using an assigned address
- Decline (DHCP Decline)
  - Sent by a client to a specific server to indicate that the assigned address is already in use
- Reconfigure (NA)
  - Sent by a server to a client to indicate that the server has new or updated configuration settings

Pour info: Messages DHCP (en anglais)

- Information-Request (DHCP Inform)
  - Sent by a client to request configuration settings (but not addresses)
- Relay-Forward (NA)
  - Sent by a relay agent to forward an encapsulated client message to a server
- Relay-Reply (NA)
  - Sent by a server to send an encapsulated server message to a client through a relay agent

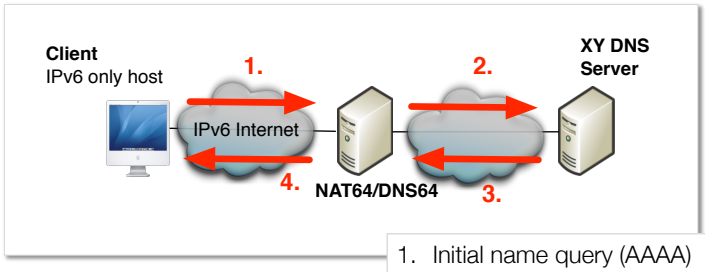
Stateful NAT64 (RFC 6146)



- Problème: comment communiquer entre un nœud IPv4 seulement et un nœud IPv6 seulement (par nom) sans faire de changement ?
- Solution:
  - DNS64 fait un mapping entre la requête de l'ordinateur IPv4 et une adresse IPv6
  - NAT64 traduit le trafic IPv6 en trafic IPv4 (adresses) et vice-versa. Aucune encapsulation. Il utilise un pool d'adresses IPv4 pour traduire les adresses IPv6 (pas besoin de pool IPv6!). La translation de port est utilisée pour économiser les adresses IPv4

Stateful NAT64 (RFC 6146)

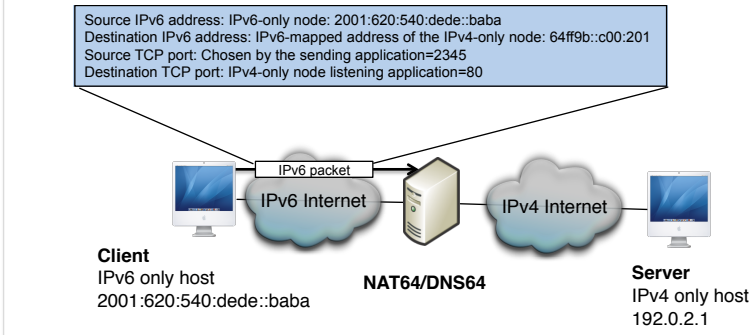
- Les routes doivent être valides sur les deux réseaux (IPv4 et IPv6)
- NAT64/DNS64 peut être configuré avec un (ou plus) préfixe valide qui soit atteignable depuis l'organisation XY



1. Initial name query (AAAA)
2. Proxied name queries (AAAA and A)
3. Name query responses (AAAA or A)
4. Constructed name query response (AAAA)

Stateful NAT64 (RFC 6146)

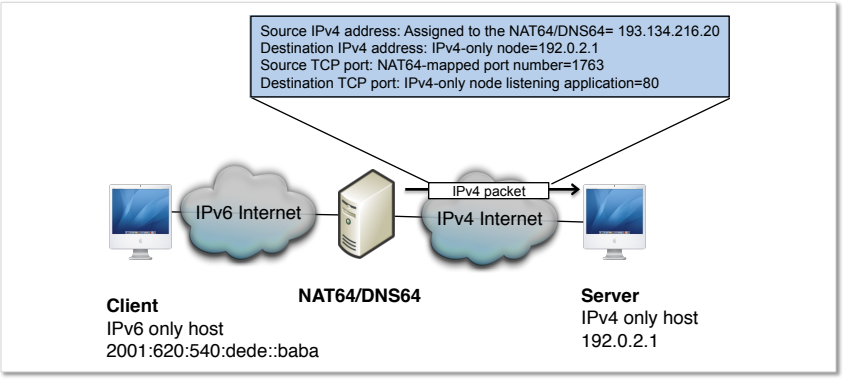
1. Paquet initial du nœud IPv6-only



- Les adresses IPv4 sont mappées avec des adresses IPv6 valides comme 64:FF9B::C00:201
- Le bloc 64:FF9B::/96 est un préfixe connu pour cet usage. D'autres préfixes peuvent être utilisés (spécifiques selon l'ISP)

Stateful NAT64 (RFC 6146)

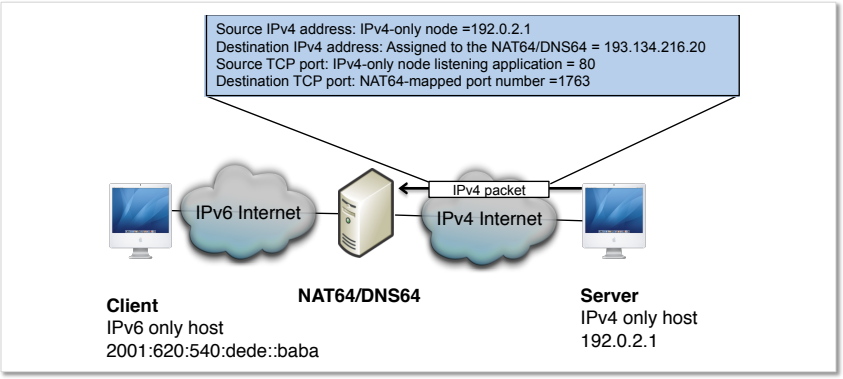
2. Paquet translaté IPv4 pour le nœud IPv4-only



- Le NAT possède le pool d'adresses 193.134.216/24
- La paquet du client est translaté par le NAT qui lui attribue la prochaine combinaison adresse/port disponible

Stateful NAT64 (RFC 6146)

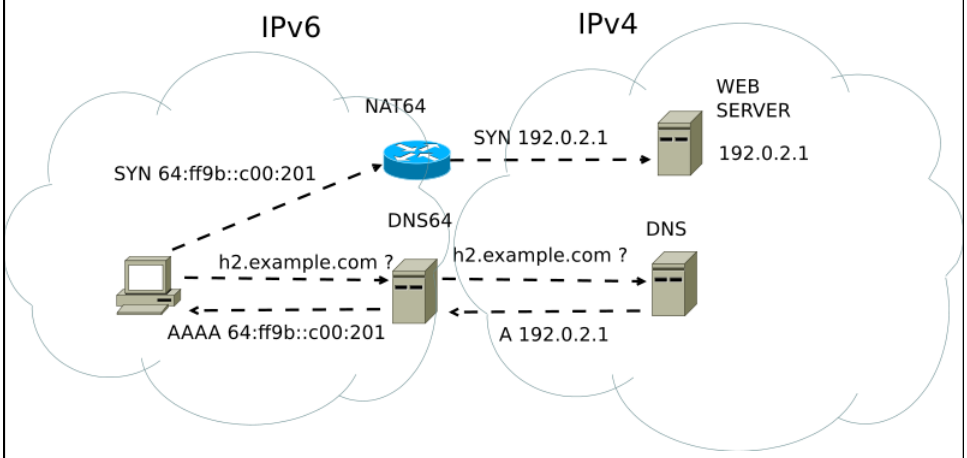
3. Réponse du nœud IPv4-only



Stateful NAT64 (RFC 6146)

4. Paquet translaté pour le noeud IPv6-only

Exemple



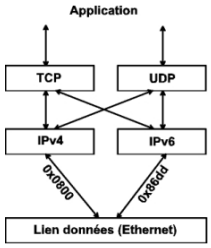
Transition vers IPv6

- Moteurs de la transition
  - Pénurie d'adresses dans les pays avec une forte croissance de l'Internet
  - Demande d'adresses pour les nouveaux types de réseaux (réseaux mobiles, réseaux domotiques)
- Obstacles
  - Pas de 'killer application' d'IPv6
    - IPv6 offre les mêmes fonctionnalités que IPv4
  - Coût de la migration
    - Mise à jour de l'équipement et des applications
    - Formation des administrateurs de réseau
  - Manque d'expérience, peur de pannes, …

➢ Processus progressive avec une longue phase de coexistence d'IPv4 et IPv6

Double pile IPv4 et IPv6

- Permet la compatibilité entre IPv4 et IPv6
- Une machine a des adresses IPv4 et IPv6
  - ➢ Un hôte double pile peut communiquer avec des hôtes IPv4, IPv6 et double pile
- Comment choisir la version d'IP d'une transmission ?
  - DNS répond à une requête avec une adresse IPv4, IPv6 ou les deux



Coexistance

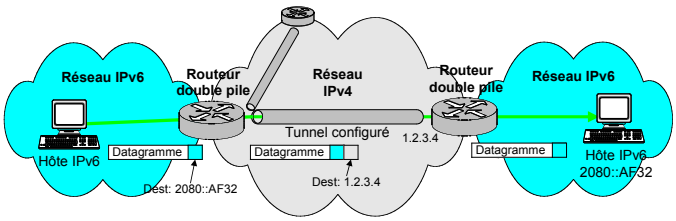
- Qu'est-ce qui doit être résolu?
- Permettre à des hôtes IPv6-only de communiquer avec des hôtes IPv4 only
  - Exemple: un nœud IPv6 veut se connecter à un serveur IPv4
- Accès « like-to-like »
  - Un hôte IPv6 veut communiquer avec un autre hôte IPv6 à travers un réseau IPv4 (exemple: Un ordinateur personnel à la maison veut se connecter à un serveur IPv6)
  - Un hôte IPv4 veut communiquer avec un serveur IPv4 à travers un réseau IPv6 (dans le futur…)

Coexistance

- Des paquets IP v6 peuvent être transportés par des paquets IPv4 (protocole d'encapsulation 41 (protocol header avec IPv4) ou vice versa avec le protocole 04)
- Variantes
  - 6to4
  - ISATAP: version simplifiée pour les intranets
  - Teredo: pour les hôtes en dual stack derrière des NAT IPv4

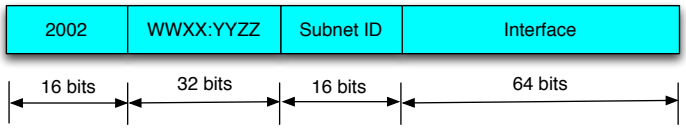
6to4 (RFC 3056)

- En principe les tunnels doivent être configurés (ce qui est pénible) mais 6to4 fourni des tunnels automatiques!



6to4 (RFC 3056)

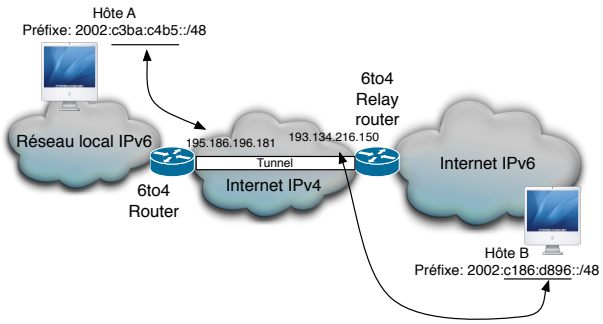
- Assignation d'adresse et tunnel automatique pour le trafic unicast entre des nœuds IPv6/IPv4 à travers le réseau IPv4
  - Les tunnels sont point-à-point, pas multicast
  - Utilisent un préfixe réservé pour 6to4: 2002::/16
  - Une adresse IPv4 externe est incluse dans le paquet
- Format du paquet:



- WWXX:YYZZ: adresse publique IPv4 en hexadecimal
  - Exemple: 193.134.216.150 est c186:d896

6to4

- Un routeur ou hôte 6to4 est capable de traiter les adresses IPv4 et IPv6 («dual stack»)



- Routeur 6to4: routeur dual stack qui peut connecter des îles IPv6 au réseau IPv4.
- Routeur relai (relay router) 6to4: routeur dual-stack qui peut connecter des internets IPv4 et IPv6.

6to4

- Lorsque l'adresse IPv4 publique du routeur 6to4 change, le réseau IPv6 doit être informé et renuméroté.
- Il n'y a qu'un point d'entrée (pas de redondance possible)
- 6to4 peut être combiné avec ISATAP

Tunnel automatique 6to4

- Les adresses 192.88.99.0 - 192.88.99.255 sont réservées pour 6to4 (6TO4-RELAY-ANYCAST-IANA-RESERVED). Chaque interface un routeur relai a une adresse IPv4 plus l'adresse anycast 192.88.99.1
- La passerelle IPv6 par défault pour le routeur 6to4 est donc 2002:c058:6301::, qui correspond à l'adresse 192.88.99.1
- Le routeur 6to4 va donc encapsuler le paquet IPv6 et va l'envoyer à l'adresse 192.88.99.1 (**tunnel automatique**)
- Le routeur relai le plus proche va recevoir le paquet et le décapsuler. Ensuite le paquet est livré à la destination.

Routeur 6to4 le plus proche depuis la maison

```
    traceroute to 192.88.99.1 (192.88.99.1), 64 hops max, 52 byte packets
 1  dsldevice.home (192.168.1.1)  1.688 ms  1.423 ms  5.085 ms
 2  131-59.186-195.fws.bluewin.ch (195.186.59.131)  23.537 ms  23.035 ms  23.126 ms
 3  10-219-3-213.bluewin.ch (213.3.219.10)  25.069 ms  25.400 ms  25.166 ms
 4  9-219-3-213.bluewin.ch (213.3.219.9)  25.729 ms  25.485 ms  25.563 ms
 5  90-218-3-213.bluewin.ch (213.3.218.90)  24.851 ms  24.872 ms  24.949 ms
 6  1-220-3-213.bluewin.ch (213.3.220.1)  25.412 ms  25.291 ms  32.591 ms
 7  2-220-3-213.bluewin.ch (213.3.220.2)  32.450 ms  28.754 ms  27.961 ms
 8  i62bsw-025-bun6.bb.ip-plus.net (138.187.129.245)  27.474 ms  29.571 ms  27.659 ms
 9  i00sto-015-ten3-1.bb.ip-plus.net (138.187.131.209)  58.160 ms  58.528 ms  57.935 ms
10  * * *
11  * * *
12  * netnod-ix-ge-a-sth-1500.alltele.se (194.68.123.183)  58.751 ms *
```

Routeur 6to4 le plus proche depuis HEIG-Vd

```
   traceroute to 192.88.99.1 (192.88.99.1), 64 hops max, 52 byte packets
1  * * *
2  193.134.216.13 (193.134.216.13)  31.373 ms  30.817 ms  30.513 ms
3  swiel2-g2-8.switch.ch (130.59.36.150)  31.453 ms  31.503 ms  31.198 ms
4  swils2-10ge-1-2.switch.ch (130.59.36.69)  33.705 ms  31.449 ms  31.579 ms
5  swibe1-10ge-1-1.switch.ch (130.59.37.130)  35.498 ms  31.925 ms  32.278 ms
6  swibe2-v300.switch.ch (130.59.36.198)  34.558 ms  32.412 ms  32.568 ms
7  swifr2-g2-3.switch.ch (130.59.36.105)  34.839 ms *  33.349 ms
```


Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

- ISATAP est une technologie de tunneling pour le trafic unicast entre deux site IPv6 à travers un réseau IPv4 (utilisé par Microsoft principalement).

  - Préfixe: Unique Local Address, Global Address ou 6to4
  - Exemple: FE80::200:5EFE:157.59.137.133

Teredo (RFC 4380)

- Pour les communications like-to-like, la solution préférée pour le tunneling est 6to4
- Problème: Ne fonctionne pas avec les NATs (sauf si les paramètres du NAT sont modifiés)
- Teredo a été inventé par Microsoft pour résoudre le problème des NAT, sans les modifier
- Utilisation de
  - Tunnels IPv6 en UDP dans IPv4
  - Routeurs relai (appelés « toredo relays »)
  - Serveurs teredo
- Les tunnels Teredo sont IP dans UDP (pas IP dans IP) pour assurer la compatibilité avec les NAT IPv4 existants

Types de NATs

- Cone NAT
  - Adresse/port interne mappé en une adresse/port externe
  - Tout le trafic interne peut être mappé en une adresse/port externe
- Restricted NATs
  - Adresse/port interne mappé en une adresse/port externe
  - Seulement valide pour un trafic spécifique
  - Le trafic venant d'une source inconnue est éliminé
- Symmetric NAT
  - Adresse/port interne + adresse/port du correspondant est mappé en une adresse/port externe

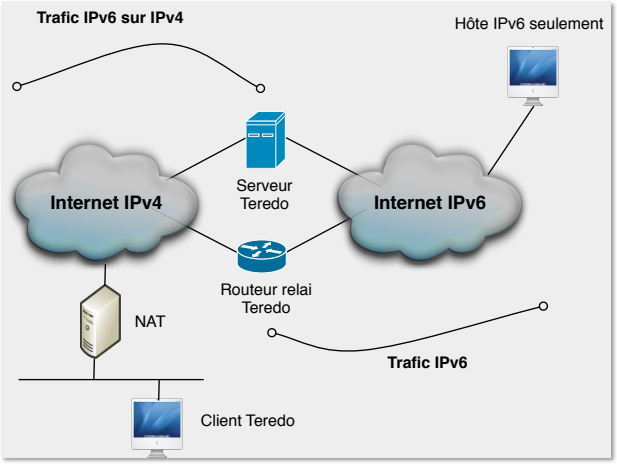
Composants Teredo

- Serveur Teredo
  - Écoute le port UDP 3544.
  - Connecté aux réseaux IPv4 et IPv6
  - Rôle: assister la configuration des adresses des clients Teredo et faciliter la communication initiale entre un client et les autres clients Teredo.Pas utilisé pour le relayage de trafic
- Routeur relai Teredo
  - Écoute le port UDP 3544.
  - Relaie tout le trafic entre IPv4 et IPv6
  - Doit être sur IPv4 et sur IPv6
  - Injecte 2001::/32 dans le routage IPv6

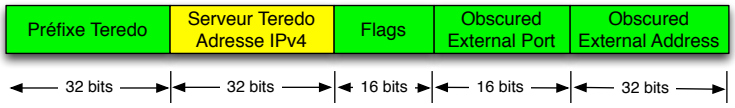
Composants Teredo

- Hôte Teredo
  - Physiquement connecté au réseau IPv4 seulement
  - A une interface IPv6 logique (interface Teredo)
  - Algorithme d'acheminement pour les paquets IPv6 à destination d'un hôte Teredo
    - Toutes les destinations Teredo sont « on-link »
    - Destinations « non Teredo »: aucune route par défault

Composants Teredo

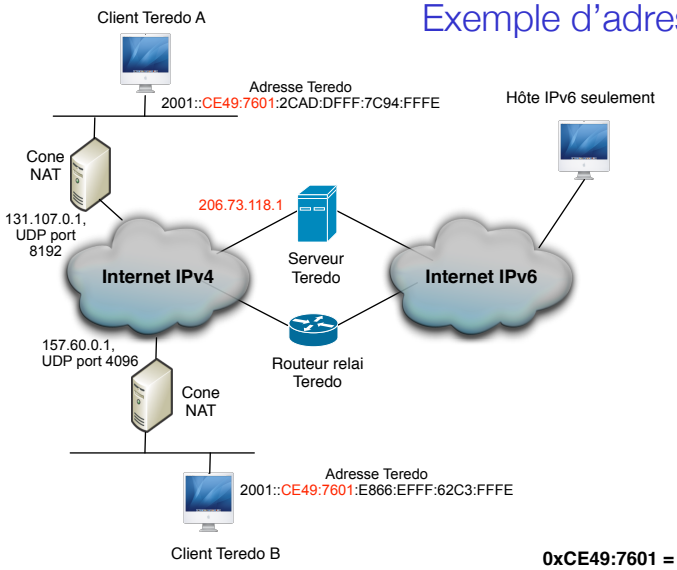


Adresses Teredo



- Préfixe Teredo: 2001::/32
- Adresse IPv4 du serveur Teredo
- Fags: drapeau de Cone (C) + bits pour l'adressage
- Obscured External Port + Address
  - XOR du port et de l'adresse externe (telle que traduite par le NAT) du host avec 0xFFF…

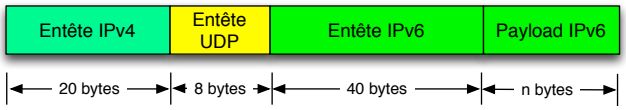
Exemple d'adressage



0xCE49:7601 = 206.73.118.1

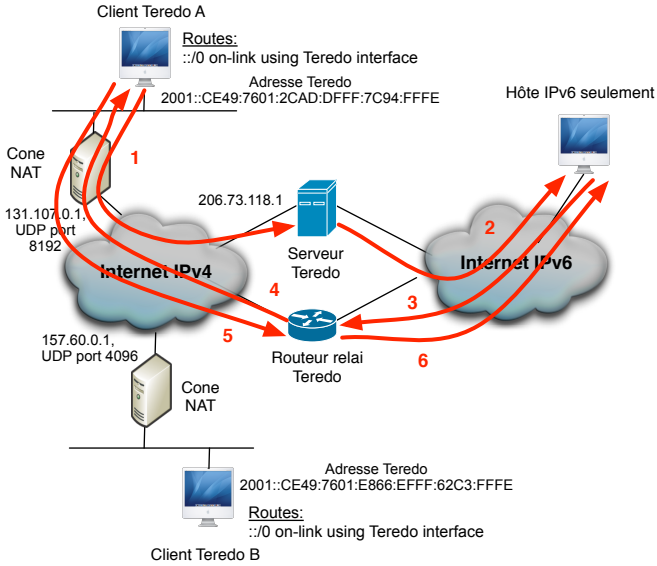
Teredo

- Format d'un paquet de données:



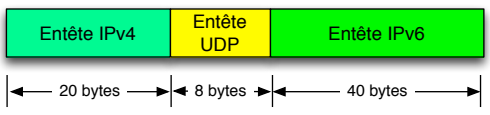
- Port du serveur Teredo: UDP 3544

Routage



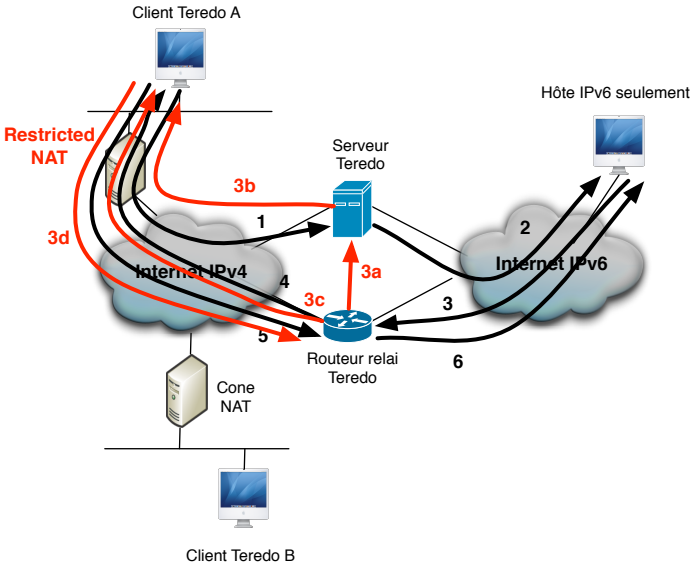
Restricted NAT

- A est derrière un NAT restreint (restricted)
  - L'adresse traduite peut être utilisée que par le serveur Teredo
  - B ne peut pas envoyer de paquet à 131.107.0.1 (les paquets seraient éliminés par le NAT)
- B sait que A est derrière un NAT restreint (à partir de l'adresse de A)
  - Le serveur achemine un « bubble » à A
  - A envoie un « bubble » à B
  - B peut envoyer des paquets à A
- Bubble:



  - Next protocol dans l'entête IPv6: 59

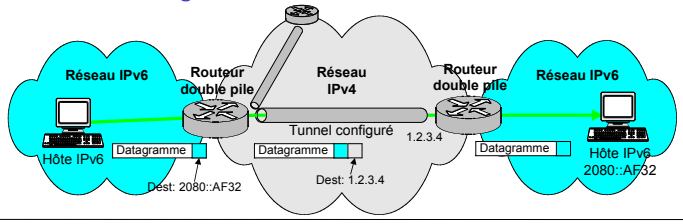
Restricted NAT



Tunnels IPv6 sur IPv4

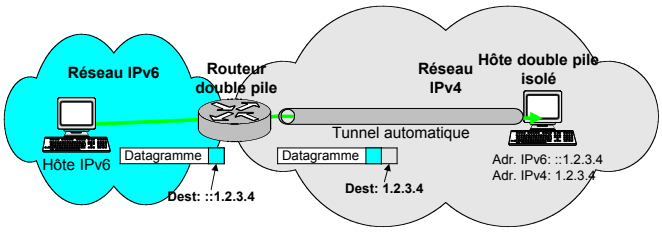
- Les réseaux de transit seront migrés progressivement vers IPv6
- L'infrastructure IPv4 restera en place
  - Routeurs double pile
- Pendant la transition il sera nécessaire de transmettre des datagrammes IPv6 des clients sur l'infrastructure IPv4

- Scénario I
  - Des îlots IPv6 sont interconnectés à travers un réseau IPv4
  - Un tunnel configuré IPv6 sur IPv4 est établi entre routeurs



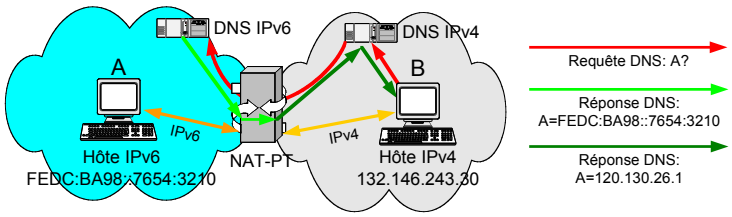
Scénario II: Tunnel automatique

- Utilisable si la terminaison du tunnel est un hôte
  - Tunnel hôte – hôte
  - Tunnel routeur – hôte
- Permet d'établir un tunnel sans configuration
- Utilise une adresse IPv6 'compatible IPv4'
  - Format 0:0:0:0:0:0:d.d.d.d
  - Conversion possible entre IPv4 et IPv6



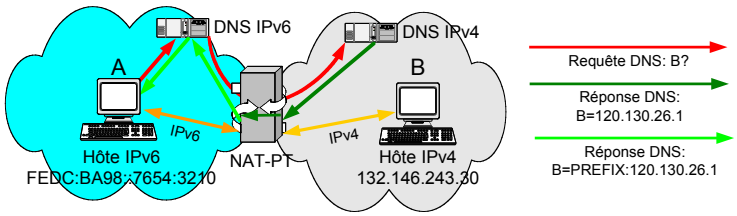
Traduction IPv4 ⇔IPv6 cont.

2. NAT-PT (Network Address Translation – Protocol Translation, RFC 2766)
   - Une passerelle NAT-PT convertit les en-têtes entre IPv6 et IPv4
   - Connexion IPv4 --> IPv6
     - B envoie requête DNS pour A
     - DNS répond avec une adresse IPv6
     - La passerelle NAT-PT intercepte la réponse DNS et assigne une adresse IPv4 temporaire à A: FEDC:BA98::7654:3210 --> 120.130.26.1
     - Ensuite communication entre B et A à travers la passerelle NAT-PT



NAT-PT cont.

- Connexion IPv6 --> IPv4
  - A envoie une requête DNS pour B
  - DNS répond avec une adresse IPv4
  - La passerelle NAT-PT intercepte la réponse DNS ajoute un préfix: 132.146.243.30 --> PREFIX::132.146.243.30
  - Lorsque A envoie un datagramme, la passerelle NAT-PT assigne une adresse IPv4 temporaire à A



Résumé IPv6

- Pénurie d'adresses --> Adresses sur 128 bit
- Croissance des tables de routage --> Adressage hiérarchique et agrégation de routes
- Acheminement à haut débit --> traitement efficace de l'en-tête IP (en-têtes d'extensions, fragmentation, …)
- Meilleure intégration des protocoles secondaires (ARP, IGMP, IP Mobile, IPSec, …)
- Fonctionnalités supplémentaires
  - Découverte de voisins (fonctionnalité d'ARP en IPv4)
  - Autoconfiguration
- Techniques de migration
  - Double pile et tunnels
  - Traduction de protocoles IPv4 ⇔ IPv6

Exercices 51, 52, 53, 54