



Internet Protocol version 6



Plan

- ⊗ Pourquoi un nouveau Protocole IP ?
- ⊗ Caractéristiques et fonctionnalités du nouvel IP
- ⊗ Structure des en-têtes IPv6
- ⊗ Formats des adresses
- ⊗ Préfixes et plans d'adressage
- ⊗ Les "nouveaux" protocoles associés à IPv6
- ⊗ Les Protocoles de routage
- ⊗ Qualité de Service
- ⊗ La mobilité IPv6
- ⊗ Sécurité

Plan (2)



- ⊗ Plan et techniques de Transition
- ⊗ l'Internet version 6 : le 6bone, G6bone ...
- ⊗ Le G6 et ses activités
- ⊗ Bibliographie et pointeurs

Contributions



Par ordre "d'entrée en scène" ...

- | | | |
|--------------------|------|------------|
| ⊗ Bernard Tuy | UREC | Paris |
| ⊗ J-Luc Archimbaud | UREC | Grenoble |
| ⊗ Alain Durand | IMAG | Grenoble |
| ⊗ Jean-Luc Richier | IMAG | Grenoble |
| ⊗ Thomas Noël | ULP | Strasbourg |
| ⊗ Laurent Toutain | ENST | Rennes |

Pourquoi un nouveau Protocole IP ?



⊗ *Actuellement la taille de l'Internet double tous les 12mois*

⊗ 2 problèmes à résoudre

- l'épuisement des adresses IP (2008 +/- 3 ans : ALE-wg)
- l'explosion de la taille des tables de routage

⊗ le nouveau protocole doit permettre

- d'adresser un espace (beaucoup) plus grand (10 E+9 réseaux au minimum)
- un routage plus efficace

de IPv4 à IPv6



⊗ Pour résoudre ces problèmes :

- **Nouvelle version** de Internet Protocol : Version 6
 - actuellement : IPv4.
 - IANA: Internet Assignment Numbers Authority (RFC 1700)

⊗ Ce nouveau protocole (IPv6) :

- garde ce qui a fait le succès de l'Internet
- étend la fonction d'adressage et de routage
- tend à résoudre les problèmes qui vont devenir critiques (applications temps réel, multipoint, sécurité...)
- cherche à faciliter la migration de IPX et OSI vers IP

=> Bon exemple d'évolution de la technologie de l'Internet

de IPv4 à IPv6(2)



- ⊗ Le rôle de l'IETF et de l'IESG :
 - le livre blanc (RFC 1550)
- ⊗ Les Propositions pour un nouveau protocole :
21 réponses ont été reçues dont :
 - CATNIP(Common Architecture for the Internet) RFC 1707
 - SIPP (Simple Internet Protocol Plus) RFC 1770
 - TUBA (TCP and UDP with Bigger Addresses)
- ⊗ RFC 1726 (déc. 1994) :
 - "Technical Criteria for Choosing IP The Next Generation"
- ⊗ RFC 1752 (Jan. 1995) :
 - "The Recommendation for the IP Next Generation Protocol"

IPv6 Quelques Caractéristiques



- ⊗ Adresse plus longue : 128 bits (16 octets)
 - adressage de 340×10^{36} équipements
 - adressage hiérarchique
 - une partie peut-être l'adresse MAC (IEEE802)
=> autoconfiguration
- ⊗ 3 types d'adresses :
 - Unicast
 - Multicast
 - Anycast

plus d'adresse de broadcast

IPv6 Quelques Caractéristiques (2)



☒ En-tête simplifié

- nombre de champs réduit de moitié
- => augmente l'efficacité de commutation des équipements de routage

☒ Extension de l'en-tête pour les options

- Les options IPv6 sont placées dans des en-têtes séparés, intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport
 - => introduction aisée de nouvelles fonctionnalités
- la longueur des options n'est plus limitée à 40 octets

IPv6 Nouvelles fonctionnalités



☒ Autoconfiguration : "*plug and play*"

- Gestion de la mobilité
- Renumerotation facile si changement de prestataire
- Serveurs d'adresses (DHCP : *Dynamic Host Configuration Protocol*) et SAA : *Stateless Address Autoconfiguration (RFC 1971)*

☒ Multipoint (*Multicast*) inclus de base

- pour les routeurs et les clients
 - "scope" = meilleur routage des paquets multicast
- => plus besoin de Mbone ni de mrouterd

IPv6 Nouvelles fonctionnalités (2)



☒ "Marquage" des flux particuliers : (*Flow Label*)

- applications temps réel, Qualité de Service (QoS)
- Priorité du trafic de contrôle

☒ Sécurité :

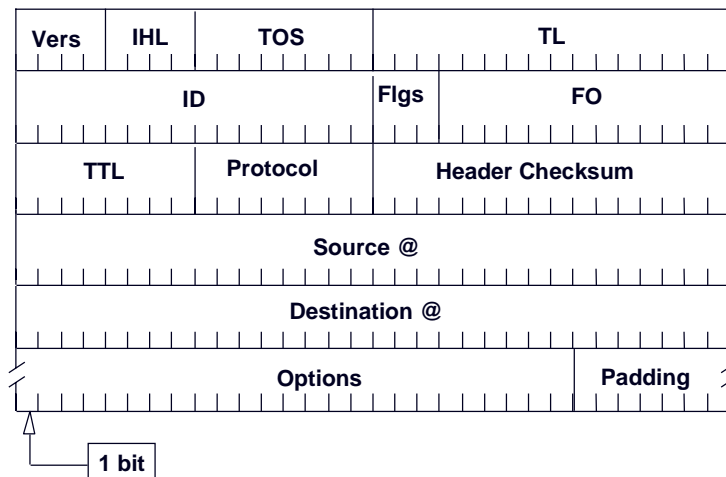
- authentification et intégrité des données
- *en option* : confidentialité

☒ Routage à partir de la source

- Source Demand Routing Protocol

IPv4

En-tête



IPv4 -> IPv6

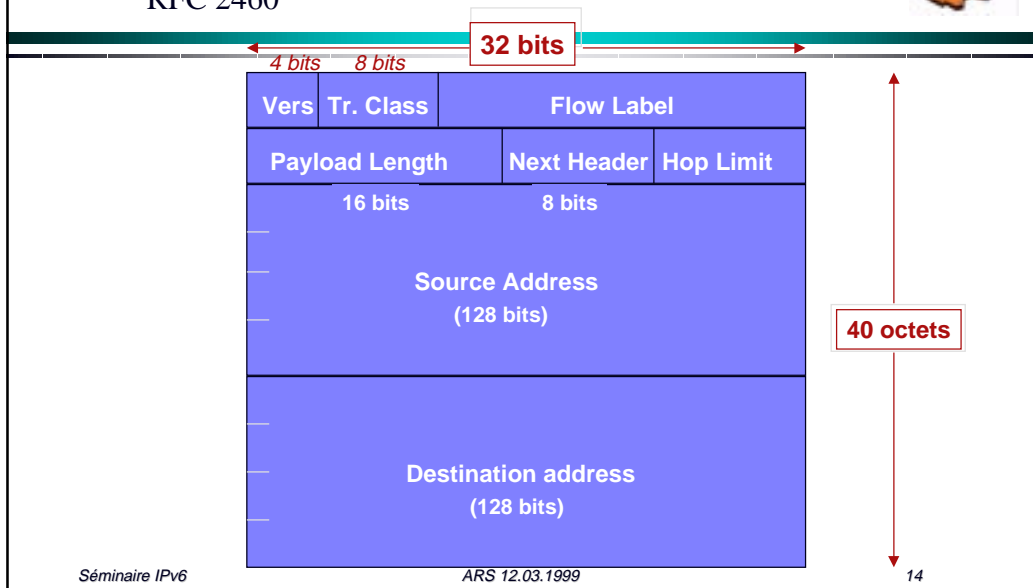
changements de l'en-tête



- ⊗ Header Length (IHL) : supprimé
- ⊗ ToS --> Flow Label
- ⊗ Total Length (TL) --> Payload Length
- ⊗ ID, Flags et Fragment Offset (FO) : supprimés
- ⊗ TTL --> Hop Limit
- ⊗ Protocol --> Next header (mêmes valeurs que dans IPv4)
- ⊗ Header CS : supprimé
- ⊗ Adresses : 32 --> 128 bits (4 --> 16 octets)
- ⊗ Alignement 32 --> 64 bits

IPv6 RFC 2460

En-tête



IPv6 les champs de l'en-tête

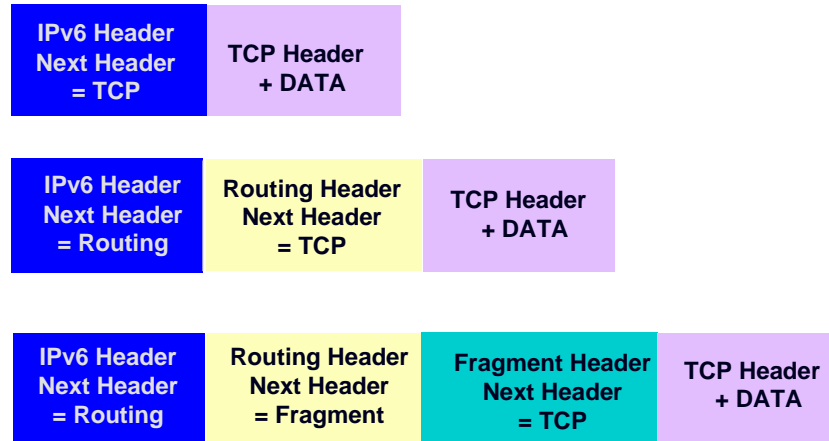


- ⊗ Vers : Version Number (= 6)
- ⊗ Traffic Class : priorité ou classes de trafic (Differentiated Services)
- ⊗ Flow label : marquage des paquets «spéciaux»
- ⊗ Payload length : longueur du paquet après en-tête (en octets).
 - autorise des paquets > 64 Koctets
 - => Payload length = 0
 - + longueur du paquet dans l'en-tête de l'option "Hop-by-hop"
- ⊗ Next header : indique le type d'entête suivant immédiatement l'entête IPv6
 - On utilise les mêmes valeurs que dans le champ "Protocol" de IPv4 pour référencer les protocoles de niveau 4 (TCP=6 , UDP=17, ICMP=1)

IPv6 les champs de l'en-tête (2)



- ⊗ Hop limit :
 - -1 chaque fois que le paquet est commuté par un équipement
 - si hop_limit = 0 => le paquet est détruit.
 - permet de réduire l'effet des boucles de routage.
- ⊗ Source address : @ de l'émetteur initial du paquet
- ⊗ Destination address : Une adresse de destination ...
 - peut-être différente de l'adresse destination finale si l'option "Routing Header" est présente.



- ⊗ Hop-by-Hop Header :
 - transport d'information qui doit être examinée sur chaque noeud du chemin suivi par le datagramme IP.
- ⊗ End-to-end Header :
 - transport d'information qui n'est à examiner que par le destinataire du datagramme.
- ⊗ Routing Header :
 - routage à partir de la source
 - liste un ou plusieurs noeuds intermédiaires "à visiter" au cours de l'acheminement du datagramme
 - "Reverse bit" :
 - si = 1 => utiliser l'information de routage pour le retour
 - sinon => résoudre le routage à partir de l'extrémité destinataire



☒ Fragment header :

- envoi de paquets plus long que le MTU
 - Maximum Transmission Unit : 512 -> 1500 octets
 - minimum : MTU = 576 octets.
- *nota* : dans IPv6, la fragmentation n'est réalisée que par la source.

☒ Authentication Header :

- authentification et intégrité des données

☒ Privacy Header :

- chiffrement des données à protéger
 - datagramme TCP/UDP ou datagramme IPv6 entier, à la demande



☒ Allocation initiale des adresses : # 15%

- @ Unicast des prestataires de connectivité (*ISP*)
- @ Multicast
- @ à usage local
- @ compatibles IPv4
- autres : ISO NSAP, IPX, téléphone ?

☒ Réserve pour la croissance : # 85%

Allocation des Adresses de tests



- ☒ Sans connectivité à l'extérieur de la plate-forme
 - Utilisez des adresses link local (RFC 2373)

- ☒ Avec connectivité à l'extérieur (G6bone, 6bone, ...)
 - demander un préfixe de tests à un « prestataire »
Point d'Interconnexion Régional IPv6 (cf. le G6bone)
<http://www.urec.cnrs.fr/ipv6/France-tests2.html>

Allocation des adresses officielles



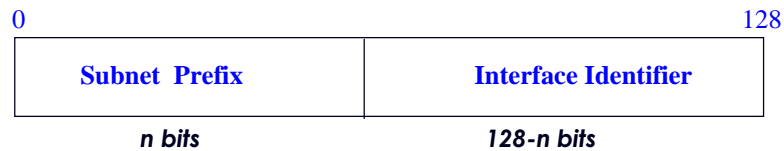
- ☒ Devrait commencer en T3-99
- ☒ Document en version finale (Internet Draft, Avril 1999)
- ☒ les RIRs vont obtenir un TLA de ICANN
- ☒ et commencer à allouer des sub-TLA
- ☒ Pour les sites/labos/entreprises :
demander à un « prestataire » IPv6
- ☒ Le G6 en substitut de Renater pour la phase de démarrage

Les Types d'adresses IPv6

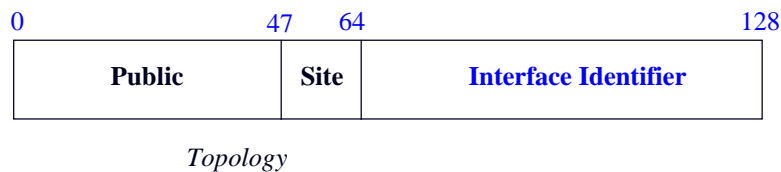


- ☒ Adresses Globales Unicast
- ☒ Adresses Multicast
- ☒ Adresses Anycast
- ☒ Adresses Site local
- ☒ Adresse Link local
- ☒ Adresses « spéciales »
 - compatibles IPv4
 - IPv4 « mappées »
 - loopback
 - non spécifiée

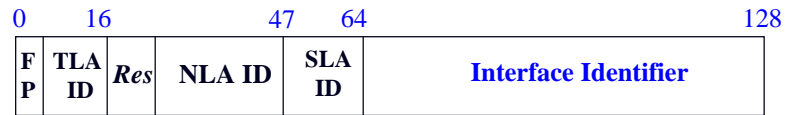
Format des adresses IPv6 RFC 2373 & 2374



Dans le plan d'adressage agrégé, n=64



Adresses Unicast globales RFC 2373 & 2374



| | |
|---|---------|
| FP : Format Prefix (001= plan agrégé; 010 = tests) | 3 bits |
| TLA ID : Top Level Aggregator | 13 bits |
| <i>Res.</i> : Reserved | 8 bits |
| NLA ID : Next Level Aggregator | 24 bits |
| SLA ID : Site Level Aggregator | 16 bits |

Identifiant d'interface (IID)



- ☒ MAC address (IEEE-802) = 48 bits
- ☒ => EUI-64 address = 64 bits
- ☒ IID = EUI-64
- ☒ Exemple :
 - MAC address = 00:A0:24:E3:FA:4B (24+24)
 - EUI-64 = 02A0:24FF:FEE3:FA4B (24+40)

02A0:24

FF:FEE3:FA4B

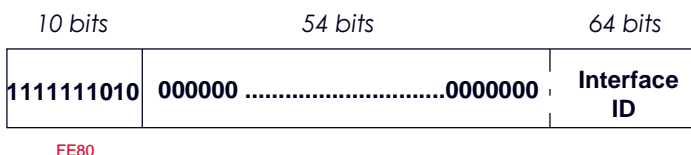
Code Constructeur
24 bits

No de Série
40 bits

Adresses Link local et Site local



Adresse link local



FE80

Adresse site local

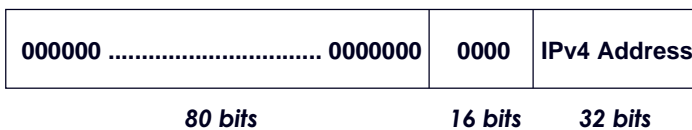


FEC0

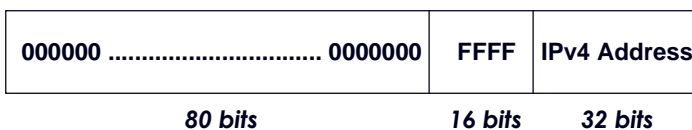
Adresses « IPv4 » (transition)



Adresse compatible IPv4 :



Adresse IPv4 "mappée" :



Adresses NSAP et IPX



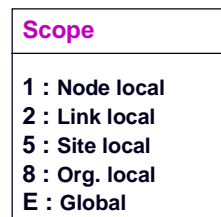
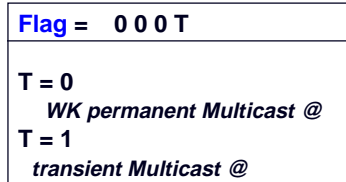
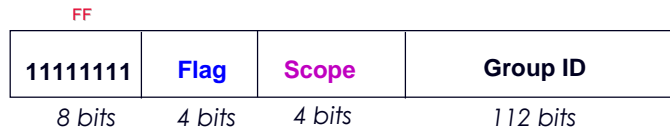
Adresse "NSAP" :



Adresse "IPX" :



Adresses Multicast



Représentation des adresses



RFC 2373

☒ Format de Base (16 octets):

- Adresse IPv6 Globale :
 - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

☒ Format compressé :

- FF01:0:0:0:0:0:43 => FF01::43
- Adresse Link Local :
 - FE80::*IID* *IID*=@ *IEEE-802*
- Adresse compatible IPv4 :
 - 0:0:0:0:0:0:134.157.4.16 => ::134.157.4.16

IPv6 : Adresses particulières



☒ Adresse de Loopback :

- 0:0:0:0:0:0:0:1 => ::1

☒ Adresse non spécifiée :

- 0:0:0:0:0:0:0:0 => ::
Ne peut jamais être adresse destination

IPv6 : Préfixes



- ⊗ Notion issue de CIDR
- ⊗ On les note sous la forme :
Adresse IPv6 / longueur du préfixe
 - Exemples :
3F00::/8
3FFE:B500::/32
- ⊗ On peut indiquer qu'une adresse fait partie d'un réseau dont le préfixe est de longueur déterminée (netmask)
3FFE:304:101:7B:22::1 /80

Plans d'adressage IPv6...



- ⊗ Géographique : abandonné
- ⊗ Prestataire : abandonné
- ⊗ GSE : abandonné
- ⊗ Agrégé : standardisé (RFC 2374)
déployé dans le 6bone
sera déployé dans les réseaux opérationnels

Préfixes et plan d'adressage agrégé



⊗ 48 (3+13+8+24) bits

topologie publique

⊗ 80 (16+64) bits

topologie privée (site)

| | | | | | |
|--------|---------|--------|---------|---------|--------------|
| 001 | TLA | Res | NLA | SLA | Interface ID |
| 3 bits | 13 bits | 8 bits | 24 bits | 16 bits | 64 bits |

Préfixes :

TLA = /16

NLA = /48

SLA = /64

— « Frontières » fixes

Préfixes de tests



| | | | | | |
|--------|---------|--------|---------|---------|--------------|
| 001 | TLA | pTLA | pNLA | SLA | Interface ID |
| 3 bits | 13 bits | 8 bits | 24 bits | 16 bits | 64 bits |

pTLA : pseudo TLA

pNLA : pseudo NLA

Plan d'adressage agrégé de test



- ⊗ 3FFE::/16 TLA délégué au 6-bone
- ⊗ 3FFE:xy::/24 pTLA délégué a chaque nœud du backbone

Exemple : 3FFE:0300::/24 pTLA délégué au G6-bone

- ⊗ charge à ce noeud de déléguer des sous-préfixes :
 - 3FFE:0304::/32 pour une "entité" (*région ou organisme*)
 - 3FFE:0304:0105::/48 pour un "site" (*ici le LIP6*)

Nouveaux Protocoles



Nouvelles fonctionnalités spécifiées dans le protocole IPv6

- ⊗ (RFC 1752 et RFC 1883)
- ⊗ Neighbor Discovery (ND)
 - RFC 2461
- ⊗ Autoconfiguration
 - Stateless Address Autoconfiguration (RFC 2462)
 - DHCPv6 :Dynamic Host Configuration Protocol Path MTU discovery (pMTU)
 - RFC 1981
- ⊗ Router Renumbering
 - encore a l'état d'Internet Draft (-08.txt, Mars 1999)

Neighbor Discovery



Les équipements IPv6 partageant le même support physique (link) utilisent Neighbor Discovery (ND) pour :

- découvrir leur présence mutuelle
- déterminer les adresses de niveau 2 des voisins
- localiser les équipements de routage
- maintenir l'information d'accessibilité vers les voisins (NUD)
- N'est pas -encore- utilisable pour les réseaux NBMA (Non Broadcast Multi Access networks)
=> ND utilise le multicast pour certains de ses services.

Neighbor Discovery



⊗ Fonctionnalités du protocole :

- Router discovery
- Prefix(es) discovery
- Parameters discovery (link MTU, Max Hop Limit ...)
- Address autoconfiguration
- Address resolution
- Next Hop determination
- Neighbor Unreachability Detection
- Duplicate Address Detection
- Redirect

Neighbor Discovery : Comparaison avec IPv4



⊗ c'est la synthèse de :

- ARP
- R-Disc
- ICMP redirect
- ...

Neighbor Discovery



⊗ ND spécifie 5 types de paquets ICMP :

- Router Solicitation (RS) :
 - un équipement requiert un RA tout de suite
- Router Advertisement (RA) :
 - Annonce (périodique) de la présence d'un routeur contient :
 - la liste des préfixes utilisés sur le lien local (autoconf)
 - une valeur possible de Max Hop Limit (TTL de IPv4)
 - et la valeur du link MTU

Neighbor Discovery (2)



- Neighbor Solicitation (NS) :
 - pour déterminer l'@ de niveau 2 d'un voisin
 - ou vérifier son accessibilité
 - également utilisé pour la DAD
- Neighbor Advertisement :
 - en réponse à une NS
 - ou pour annoncer un changement d'adresse
- Redirect :
 - utilisé par un routeur pour informer d'un meilleur chemin

Autoconfiguration à mémoire d'état (stateful)



⊗ DHCPv6 : *Dynamic Host Configuration Protocol*

- s'appuie sur le protocole BOOTP (RFC 951)
- et la version IPv4 de DHCP (RFC 1541)
- *toujours en Internet Draft (-14.txt, Février 1999)*

⊗ le serveur

- mémorise l'état du client
- fournit les @IPv6 et des paramètres de configuration du client

⊗ le client

- émet des requêtes et des "acquittements" (selon le protocole DHCP)

Autoconfiguration sans état (*stateless*) (RFC 1971)

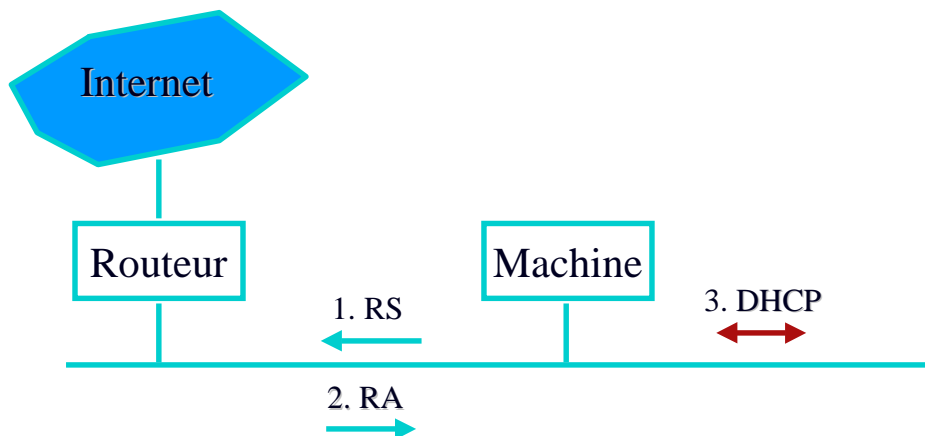


Construire une adresse globale à partir de :

- l'adresse MAC de la machine
- des annonces de préfixes faites par les routeurs sur le même lien

=> *Ce mécanisme ne s'applique pas aux routeurs
(cf. Router Renumbering)*

Auto-configuration



Path MTU discovery



RFC 1981

- ⊗ dérivé du RFC 1191, version IPv4 du Protocole
- ⊗ Path = ensemble des liens traversés par un paquet IPv6 entre la source et la destination (chemin)
- ⊗ link MTU = taille maximale de l'unité de transmission -un paquet- (en octets) qui peut être transportée sans fragmentation sur le lien
- ⊗ Path MTU (ou pMTU) = $\min \{ \text{link MTU} \}$ pour un Path donné
- ⊗ Path MTU Discovery = découverte automatique du pMTU pour un Path donné

Path MTU discovery(2)



- ⊗ Que fait le protocole ?
 1. On fait l'hypothèse que $\text{pMTU} = \text{link MTU}$ pour atteindre un voisin (first hop)
 2. S'il y a un équipement intermédiaire dont $\text{link MTU} < \text{pMTU}$
=> émission d'un message ICMPv6 : "Packet size Too Large"
 3. La source réduit le pMTU en utilisant l'information contenue dans le message ICMPv6

« Qualité » de Service



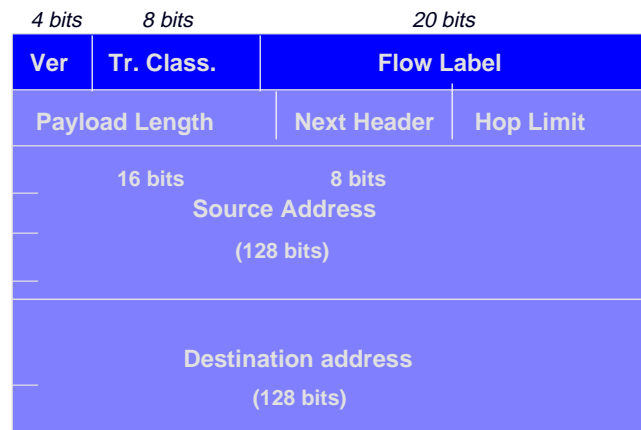
- ⊗ Besoin de différencier / garantir certains flux
- ⊗ Supports pour la QoS/CoS :
 - champ “identifiant de flux”
 - champ “priorité”⇒ Utiles pour MPLS et la réservation de ressources (RSVP)...
- ⊗ Toujours un problème ouvert :
 - mise en oeuvre dans les routeurs
 - correspondance avec les QoS d’ATM

Différenciation de services

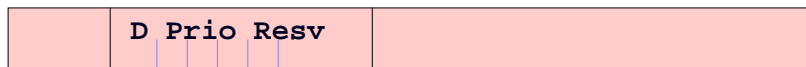


- ⊗ Garder le principe du Best-Effort, mais :
- ⊗ Offrir plus de bande passante suivant l’abonnement choisi.
- ⊗ Intérêt :
 - entreprise : meilleurs temps de réponses
 - fournisseur : demande forte des clients, meilleure rentabilisation de l’infrastructure.
- ⊗ Utilisation des techniques développées avec RSVP

En-tête IPv6 (RFC 2460)



Définition Expérimentale du champ *traffic class*



- ⊗ Bit D (1 bit) : privilégie le délai par rapport au débit
- ⊗ Prio (3 bits) : définition de la priorité pour la remise des paquets
- ⊗ Réserve (4 bits) :
 - Ex.: bit « CLP » : en cas de non respect d'un contrat de trafic

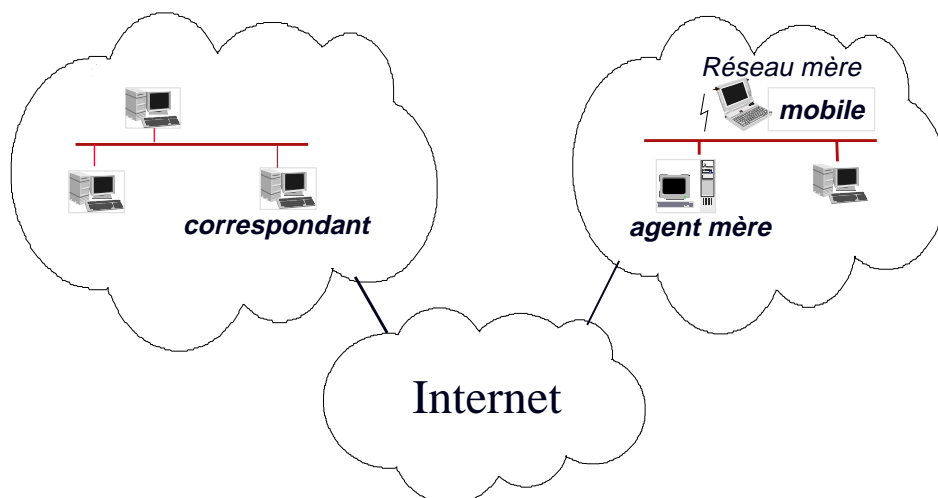


La mobilité IPv6 s'appuie sur :

- ⊗ L'expérience acquise dans IPv4
- ⊗ Les nouvelles fonctionnalités d'IPv6
- ⊗ L'opportunité du déploiement d'une nouvelle version d'IP

La mobilité IPv6 permet le support des communications avec un mobile en effectuant un routage soit :

- ⊗ vers le point d'attachement du mobile sur l'Internet
- ⊗ vers l'adresse du mobile dans son sous-réseau mère



Les principales fonctionnalités de la Mobilité IPv6



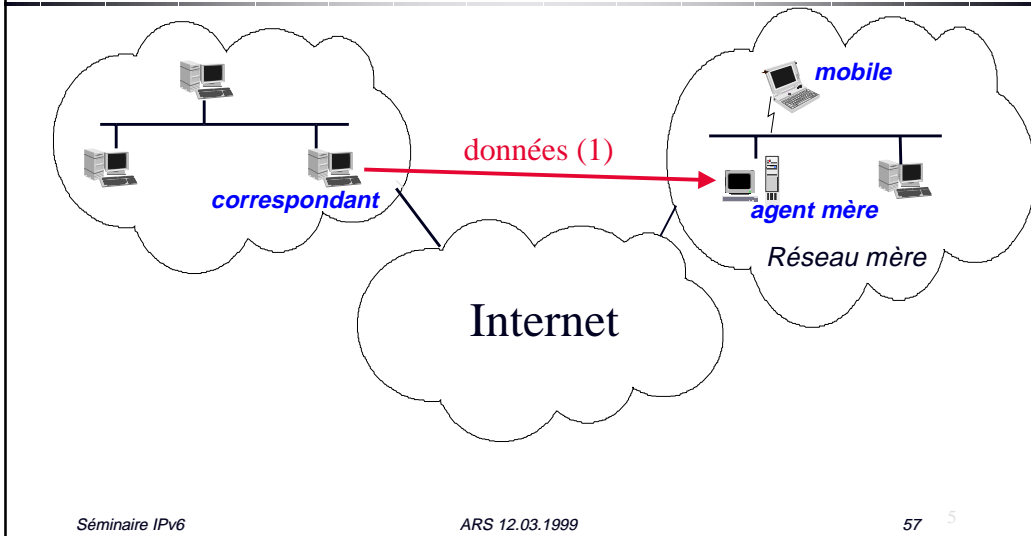
- ⊗ Les correspondants d'un mobile doivent :
 - Disposer d'une liaison dans leur cache des liaisons
 - Apprendre la position du mobile en traitant des options «Binding Update»
 - Effectuer le routage des paquets directement vers le mobile (Routing Header)
- ⊗ L'agent mère d'un mobile doit :
 - Etre un routeur dans le sous-réseau mère du mobile
 - Intercepter les paquets dans le sous-réseau mère
 - Tunneler (encapsulation IPv6) ces paquets directement au mobile

L'adressage d'un mobile

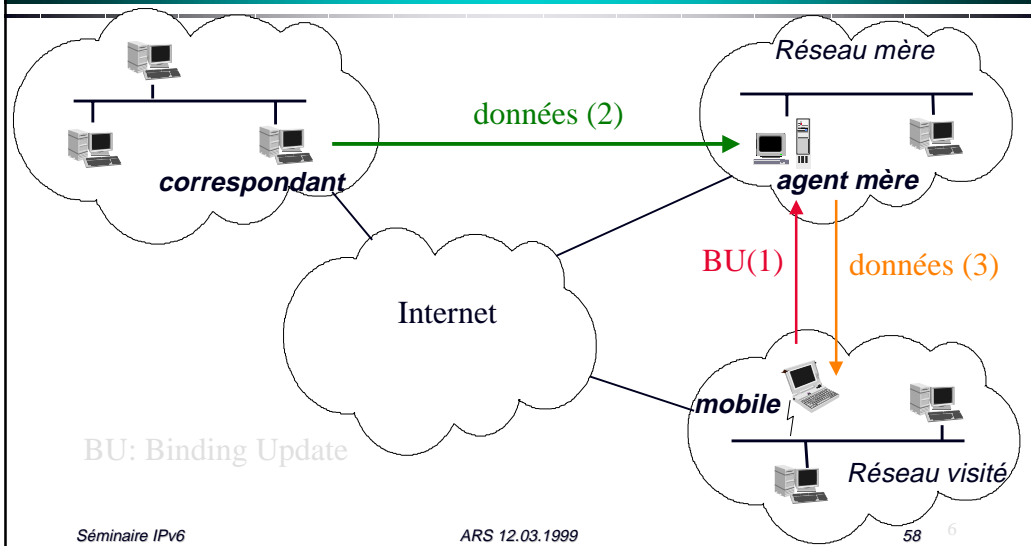


- ⊗ Un mobile est toujours *joignable* par son adresse mère
- ⊗ Un mobile en déplacement possède toujours une adresse temporaire (autoconfiguration) :
 - Réception de Router Advertisement indiquant le préfixe du sous-réseau visité
 - Concaténation de ce préfixe avec l'adresse MAC de l'interface
- ⊗ La détection de mouvement s'effectue également à l'aide des mécanismes de Neighbor Discovery

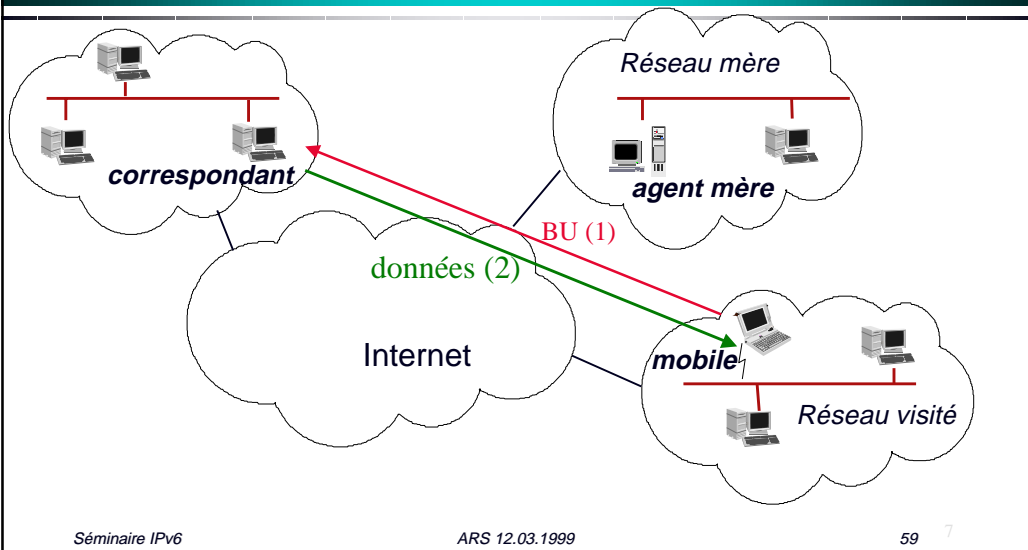
Gestion de la mobilité



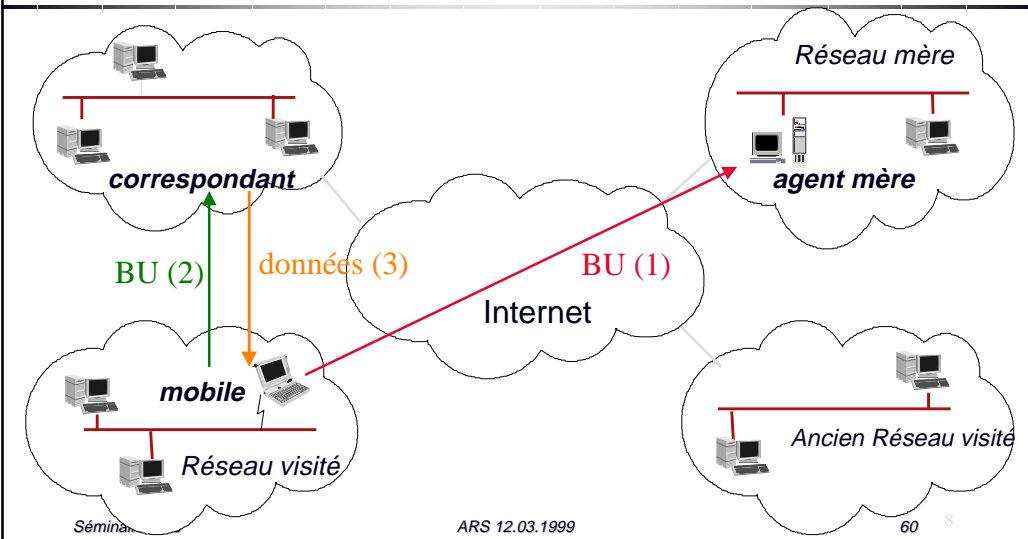
Gestion de la mobilité



Gestion de la mobilité



Gestion de la mobilité



Gestion des caches des liaisons



- ✘ Un mobile envoie à chaque déplacement un Binding Update (BU):
 - Chaque BU inclut une durée de vie
 - Un mobile maintient une liste des correspondants à qui il a envoyé un BU
 - L'adresse temporaire envoyée dans le BU destiné à l'agent mère est appelée adresse temporaire principale

Format de l'option Binding Update



- ✘ La mobilité IPv6 définit une nouvelle option destination appelée Binding Update

| | | | Option Type | Option Length |
|--|---|---|-------------|---------------|
| A | H | L | Reserved | Lifetime |
| Identification | | | | |
| Care-of Address | | | | |
| Home Link-Local Address (present only if L bit set) | | | | |

Tout paquet qui inclut l'option destination Binding Update doit également contenir un en-tête d'authentification

Le message Binding Acknowledge



- ✘ Message d'acquittement basé également sur une extension d'en-tête Destination :

| Option Type | Option Length | Status |
|----------------|---------------|--------|
| Refresh | Lifetime | |
| Identification | | |

- Envoyé uniquement si le bit A est positionné dans le Binding Update envoyé par le mobile
- Doit également utiliser un en-tête d'authentification

Fonctionnalités des Noeuds IPv6



La mobilité IPv6 demande que certaines fonctionnalités soient présentes sur tout noeud IPv6 :

- ✘ Etre capable de recevoir et traiter des Binding Update
- ✘ Envoyer des Binding Acknowledge
- ✘ Maintenir un cache des liaisons

Tout noeud IPv6 mobile doit être capable :

- ✘ D'effectuer la décapsulation IPv6
- ✘ D'envoyer des Binding Update et de recevoir des Binding Acknowledge
- ✘ De maintenir une liste des Binding Update envoyés

Fonctionnalités des routeurs IPv6



Chaque routeur IPv6 doit être capable :

- D'utiliser une entrée du cache des liaisons pour encapsuler et propager un paquet

Au moins un routeur dans le sous réseau mère d'un mobile doit être capable d'agir comme agent mère

Un agent mère doit :

- Maintenir un registre contenant la liaison avec un mobile
- Intercepter les paquets dans le sous réseau mère pour un mobile dont il a la charge
- Encapsuler ces paquets et les propager à l'adresse temporaire du mobile

Sécurité

principes



☒ RFC 2401-2411

- IPv6 et IPv4
- Authentification
- Intégrité
- Confidentialité

☒ Indépendant des algorithmes de chiffrement

- champ SAID : Security Association Identifier :
Type de clé, durée de vie, algorithme, ...

☒ Administration des clés : séparée

- ☒ Les fonctions de sécurité sont optionnelles
- ☒ elles n'affectent pas les autres utilisateurs

Sécurité authentication - intégrité



☒ Header

- Next Payload et Length (2 octets)
- Reserved (2 octets)
- SAID (4 octets)
- Donnée d'authentification ($n * 4$ octets)

☒ Résultat d'un calcul sur les données et les champs d'en-têtes qui ne changent pas (hop count ... exclus) avec une clé secrète

☒ Par défaut : MD5

☒ à utiliser de préférence entre station origine et station destination

☒ Sur les stations IPv6 : obligatoire avec MD5

Sécurité confidentialité



☒ ESP : Encapsulation Security Payload

- Inclut de fait intégrité et authentification

☒ Chiffrement de tout ou partie du datagramme

- données uniquement

☒ Ajout d'en-têtes et chiffrement du reste

- En-tête IPv6 en clair
- Autres en-têtes en clair
- En-tête ESP : SAID (en clair)
- Données chiffrées (peut inclure les en-têtes initiaux)

☒ Entre les stations ou les passerelles

☒ Support d'au moins DES CBC

- Data Encryption Standard Cipher-Block Chaining

Sécurité



- ☒ Pas de protection contre l'analyse de trafic
- ☒ Gestion des clés :
 - 2 philosophies :
 - entre utilisateurs
 - entre stations
- ☒ Station : doit supporter au moins l'affectation manuelle des clés

IPv6

Protocoles de routage



Transposition de ceux d'IPv4

- ☒ Protocoles intérieurs :
 - RIPng
 - OSPFng
- ☒ Protocoles extérieurs :
 - IDRP : abandonne
 - BGP4+ : version modifiée de BGP4 pour IPv6 adaptée au routage des datagrammes IPv6 et à la gestion des routes Multicast IPv4 (mBGP)



☒ Philosophie générale :

- Compatibilité de IPv6 avec IPv4 (postes de travail et routeurs)
- Facile à installer et faible coût initial
- Acquérir de l'expérience le plus tôt possible

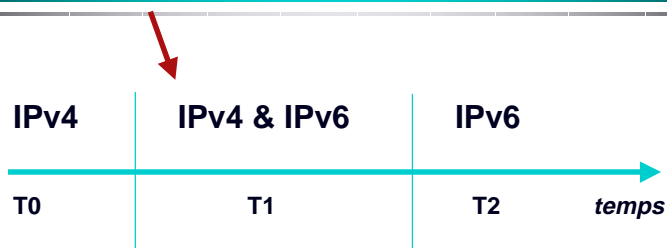
☒ Objectifs :

- Evolution progressive des machines et des routeurs : **PAS de JOUR J !!!**
- Peu ou pas de dépendances (phases multiples, état des autres équipements...)
- Terminer la transition avant l'épuisement des @ IPv4

☒ Problèmes :

- Pas d'opérateurs => pas de transition (pas de client)
- Pas de clients => pas d'opérateurs

La transition de IPv4 à IPv6



Les techniques a mettre en œuvre diffèreront selon que :

- l'équipement est double pile ou pas
- l'application est portée sur IPv6 ou pas
- le monde environnant est majoritairement IPv6 ou IPv4

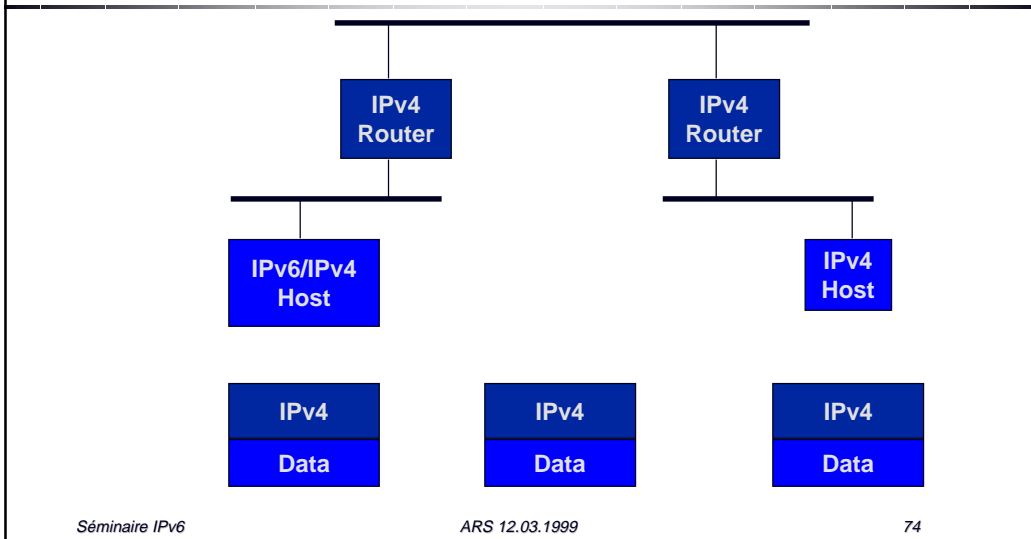
IPv6 techniques de transition



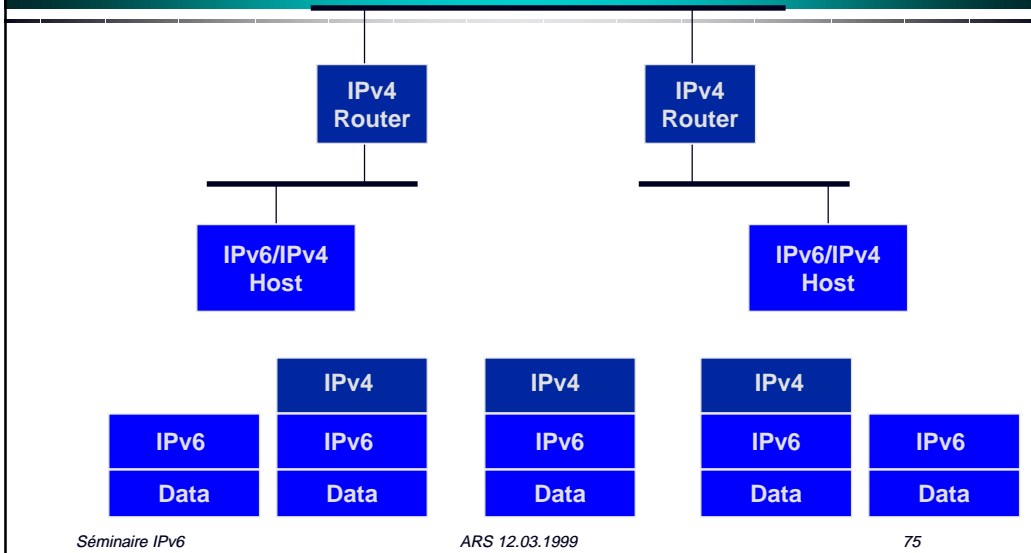
RFC 1933 + ID -03.txt (Avril 1999)

- ⊗ Double Pile logicielle (IPv6 et IPv4)
- ⊗ Encapsulation de IPv6 dans IPv4 (tunelling)
- ⊗ Traduction IPv6 <=> IPv4
Passerelles Applicatives

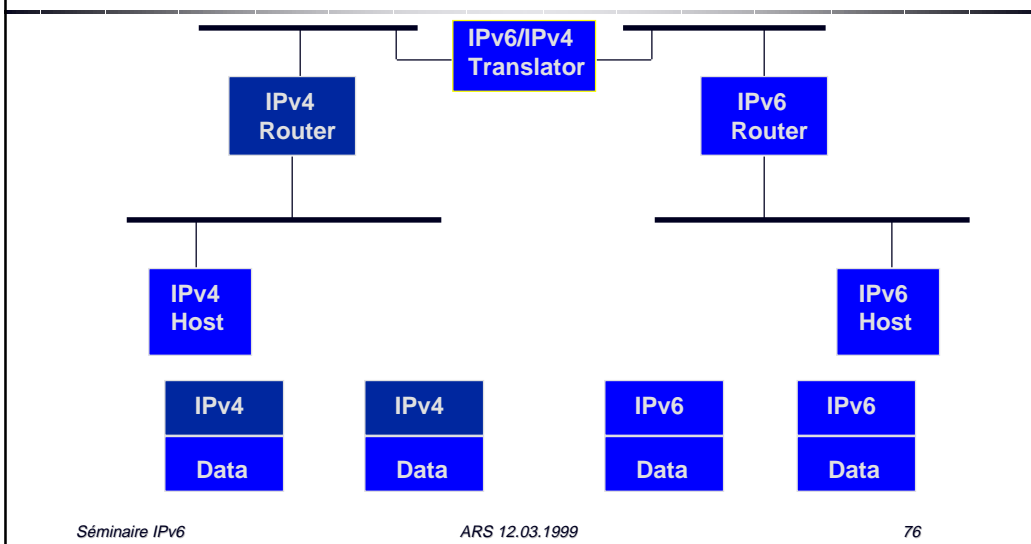
IPv6 <=> IPv4 : Interopérabilité



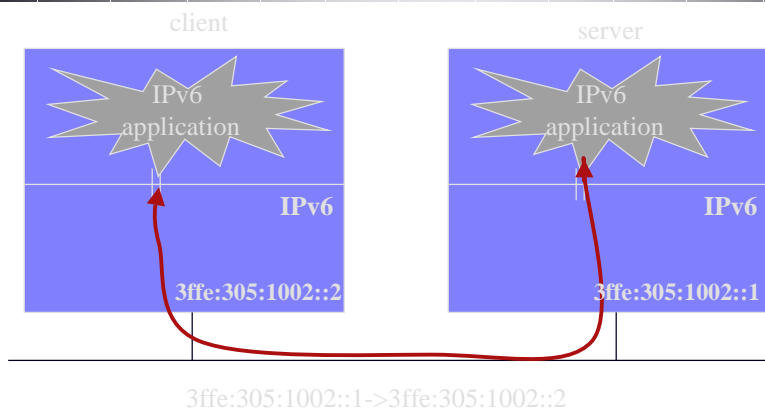
IPv6 \Leftrightarrow IPv6 : Tunneling dans IPv4



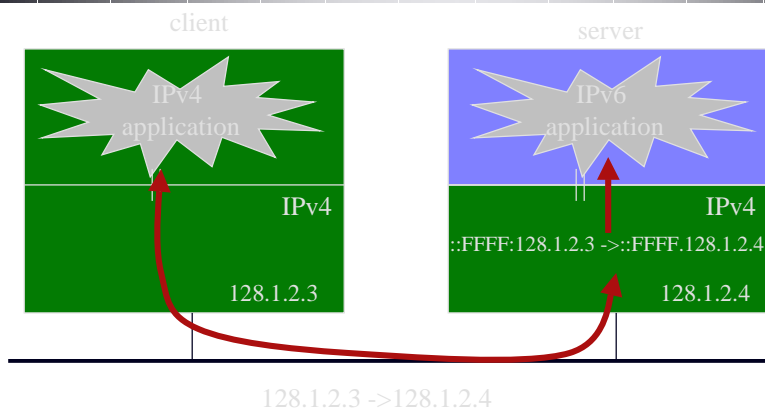
IPv6 \Leftrightarrow IPv4 : traduction en-têtes



Application IPv6 : fonctionnement usuel



IPv6 <=> IPv4 : Adresses «mappées»



IPv6 \Leftrightarrow IPv4 :

Double Pile IP



⊗ *les équipements ont une adresse dans chacun des plans d'adressage IPv4 et IPv6*

=> ils acheminent le trafic IPv4 et le trafic IPv6

⊗ *ne résoud pas le problème de pénurie des adresses IPv4*

⊗ **Applications :**

compilées pour IPv6 : utilisent les adresses IPv4 mappées

compilées pour IPv4 : utilisent les adresses IPv4

Double Pile IP :

étape ultérieure



⊗ **Allouer dynamiquement une adresse IPv4 à un équipement IPv6 quand :**

- il veut parler à un équipement IPv4
- un équipement IPv4 veut lui parler

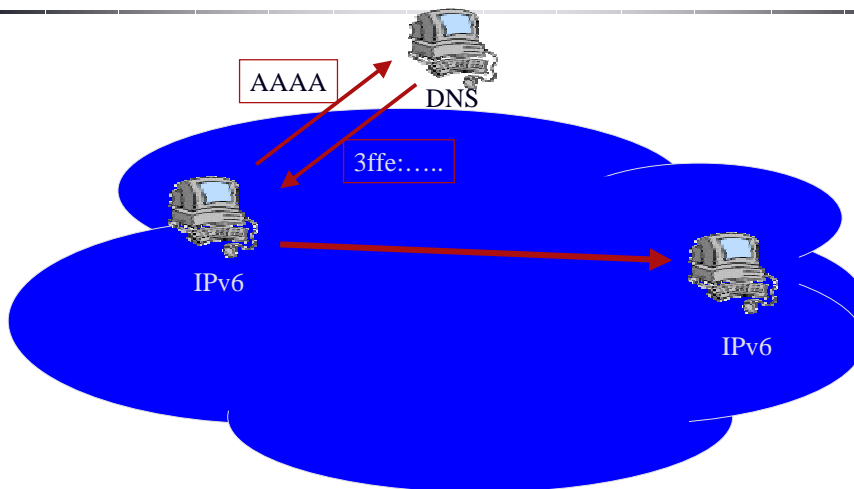
⊗ **Role central des Serveurs de Noms et DHCP**

⊗ **s'appuie sur 2 propositions en cours de normalisation**

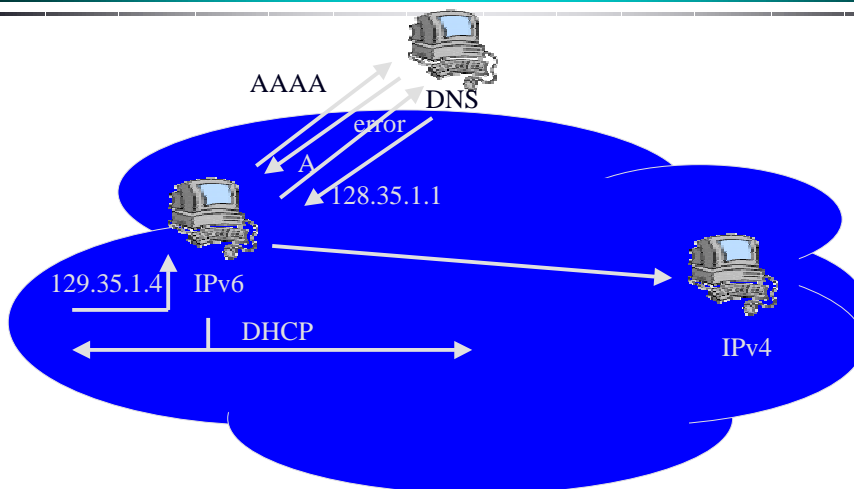
- AIIH : Assignment of IPv4 Addresses to IPv6 Hosts
- DTI : Dynamic Tunneling Interface

IPv6 <=> IPv6 :

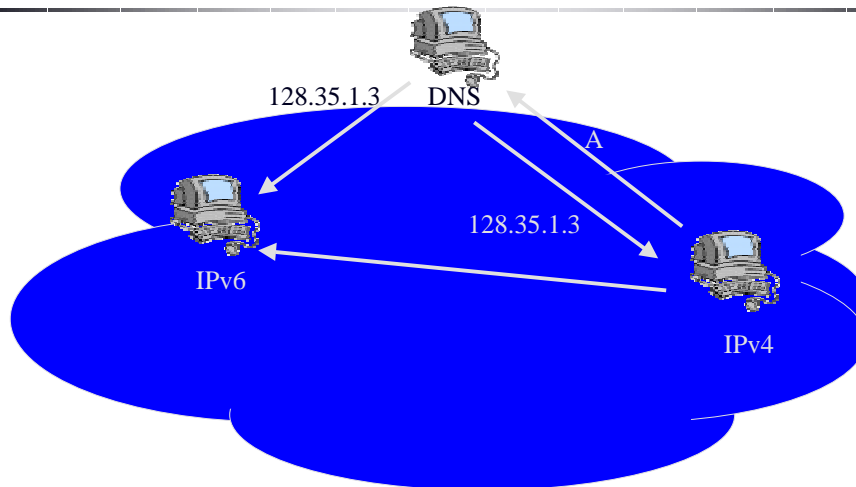
fct usuel



IPv6 => IPv4



IPv4 => IPv6



IPv6 <=> IPv6 : encapsulation v4



⊗ tunnels IPv6 à travers une infrastructure IPv4 :

- tunnels configurés :
datagrammes IPv6 + en-têtes IPv4
- tunnels automatiques :
datagrammes IPv6 avec adresses IPv4 mappées ou compatibles
l'adresse IPv4 est dérivée de l'adresse IPv6
- *un équipement peut avoir à la fois des tunnels configurés et des tunnels automatiques -ou aucun des deux.*

IPv6 <=> IPv4 : Traduction des en-têtes



Interopérabilité entre les équipements seulement IPv4 et les équipements seulement IPv6.

- Ces mécanismes redeviennent très en vogue ... avec le NATv4!

- **Internet Draft : NAT-PT** (-05.txt, Février 1999)

N'utilise pas la double pile protocolaire, mais l'allocation dynamique d'une adresse IPv4 a l'équipement IPv6.

Il établit également la correspondance entre les ports TCP/UDP IPv6 et leurs équivalents IPv4 (et vice versa)

- **Internet Draft : SIIT** (Stateless IP/ICMP Translator) (-05.txt, Janvier 1999)

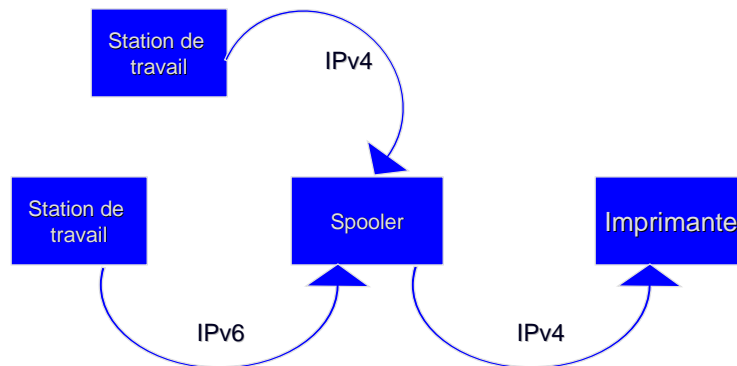
Apparaît comme une proposition simplifiée de NAT-PT

IPv6 <=> IPv4 :

ALG



ALG : Application Layer Gateway



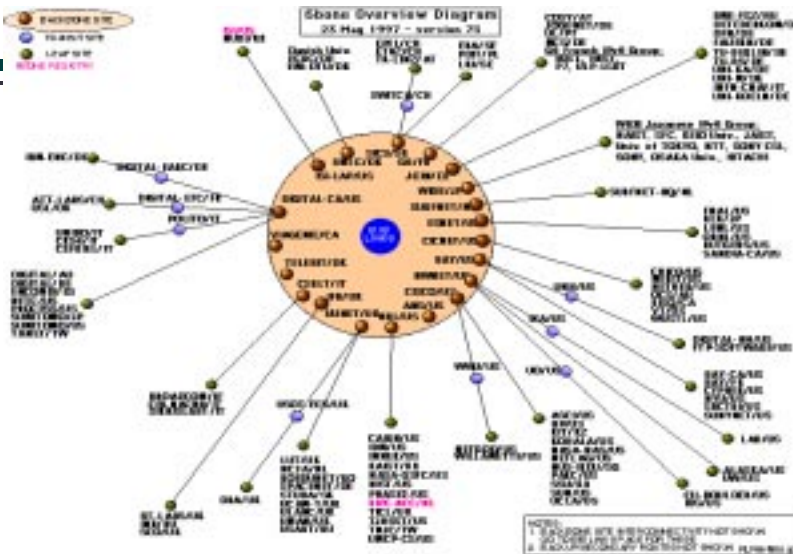
Le 6-bone



- ⊗ Réseau IPv6 expérimental construit au dessus de l'Internet IPv4 (tunnels)
- ⊗ Lancé le 15 Juillet 1996 par 3 sites (WIDE/JP, UNI-C/DK, G6/FR)
- ⊗ Aujourd'hui: 400 sites & 27 pays
- ⊗ Groupe de travail IETF
- ⊗ <http://www.6bone.net>



Carte du 6-bone (23/5/97)

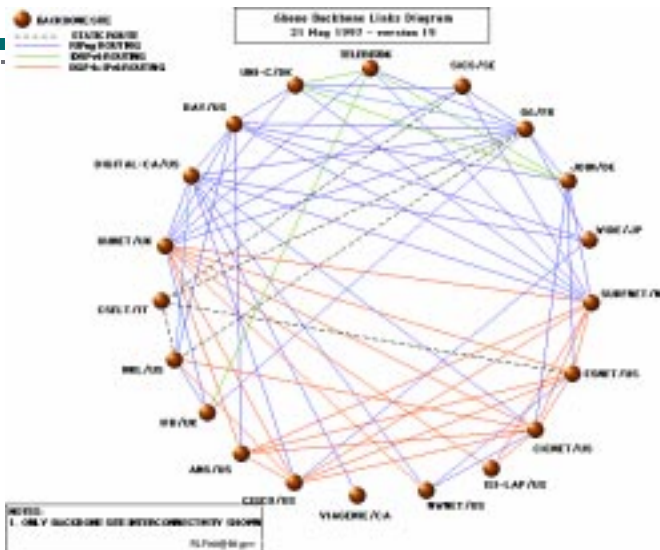


Le 6bone



- ⊗ pré-déploiement de l'Internet version 6
- ⊗ nuages de machines connectées en IPv6
- ⊗ tunnels IPv4 pour interconnecter les nuages IPv6
- ⊗ problème : le routage
 - statique (route par défaut)
 - dynamique (RIPv6 (obsolète), BGP4+, ...)
 - cœur en BGP4+

Le coeur du 6-bone (21/5/97)





- ⊗ Le 6bone est un réseau de test, pas de production
- ⊗ Aujourd'hui les standards et les implémentations existent il faut déployer
- ⊗ Les réseaux d'éducation et de recherche (REN) doivent contribuer à IPv6, comme ils l'ont fait pour le début d'Internet
- ⊗ Créer des réseaux de production IPv6 permettant d'utiliser des applications réelles
- ⊗ Le 6REN veut **promouvoir** et **cordonner** un service IPv6 de niveau production
- ⊗ Le 6REN n'est pas un réseau, c'est une coordination de réseaux

6REN



- ⊗ Début octobre 1998, ESnet a établi des « peerings » en IPv6 natif au dessus d'ATM avec CAIRN, Internet2/vBNS et CA*net2.
- ⊗ et a lancé une initiative ouverte, le 6REN, afin d'être un point de convergence pour les réseaux d'éducation et de recherche du monde entier.
- ⊗ Les réseaux Education/Recherche d'Australie et de Chine ont des projets pour fournir un service IPv6 en production à l'échelle du pays.
 - AARNET - the Australian Academic and Research Network
 - CERNET - the China Education and Research Network

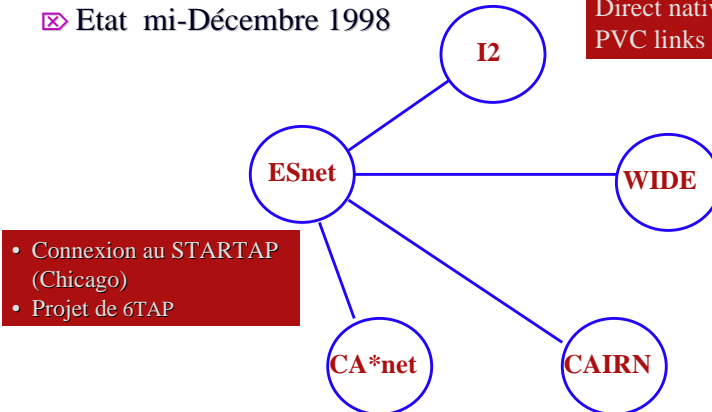


6REN actuel



⊗ Etat mi-Décembre 1998

Direct native IP over ATM
PVC links w/BGP4+ peering



Le G6



⊗ Groupe français d'expérimentation IPv6

⊗ Créé fin 1995 et animé par

- Alain Durand, IMAG (CNRS/Université)
- Bernard Tuy, UREC (CNRS)

⊗ Regroupe des académiques et des industriels :

- CNRS, ENST, INRIA
- Universités de Paris 7, Strasbourg ...
- Bull, Dassault électronique, Eurocontrol ...

Charte du G6

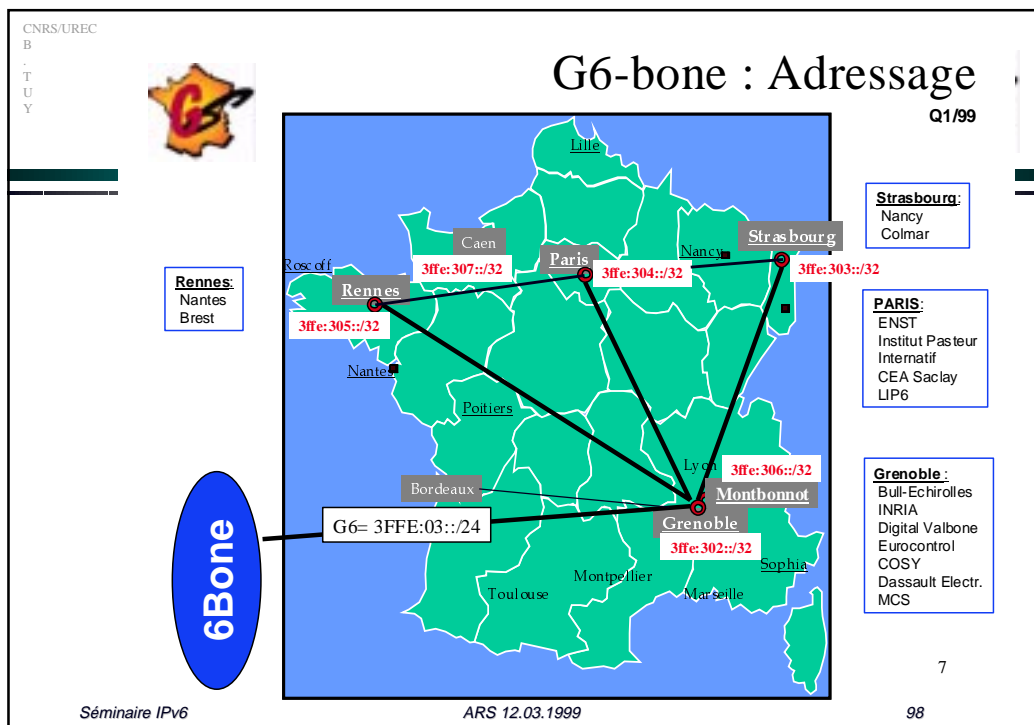
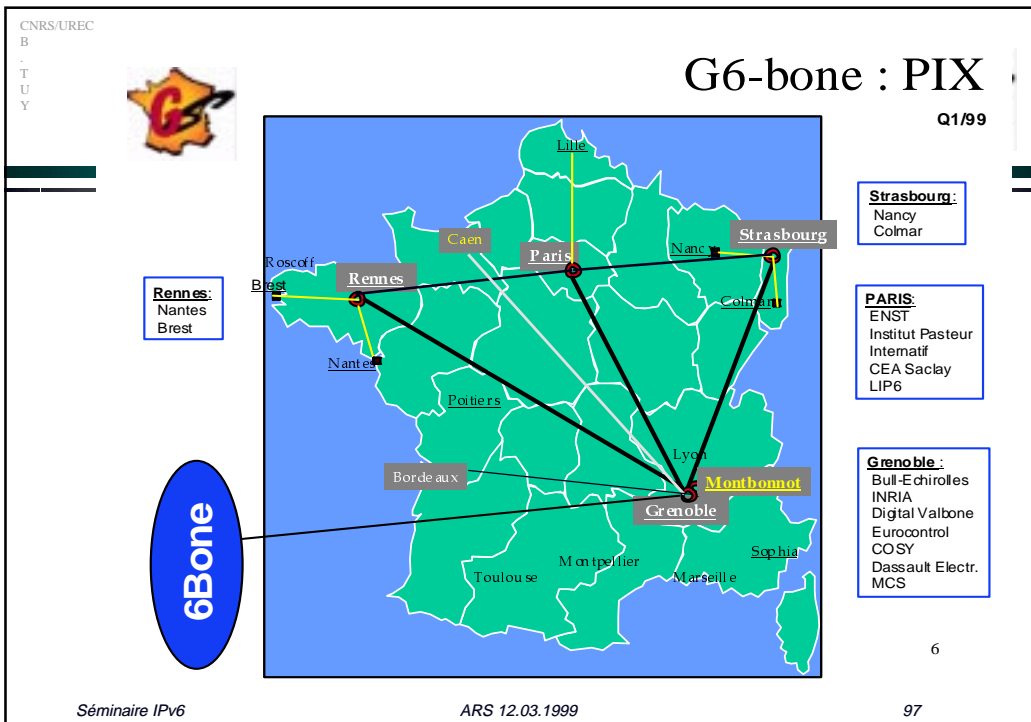


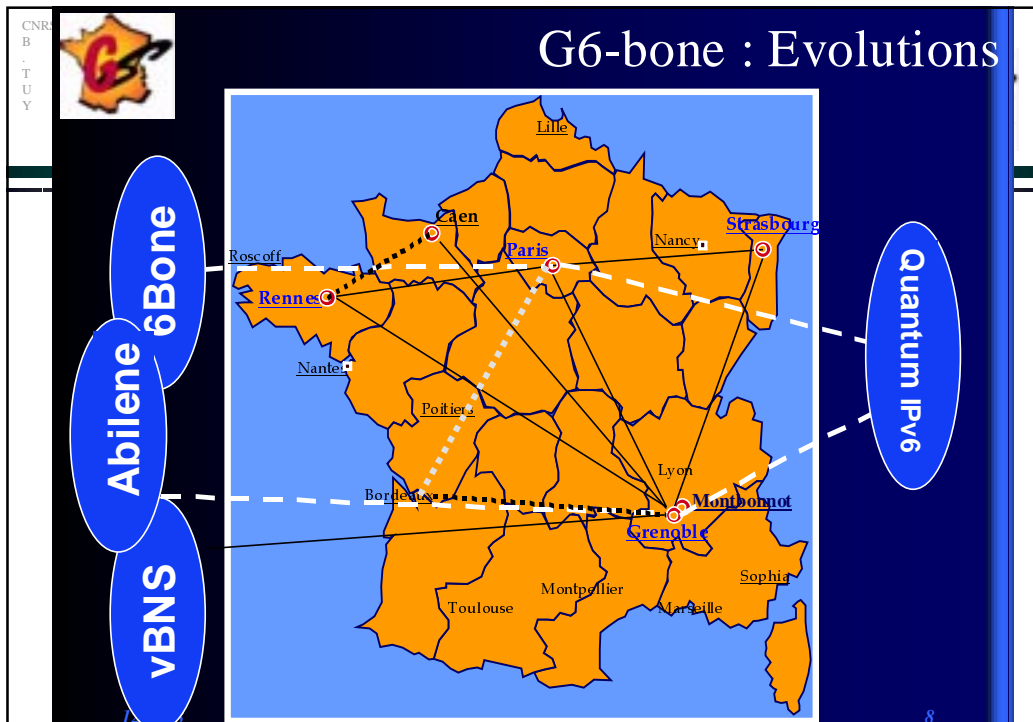
- ⊗ Echanges d'expérience
- ⊗ Diffusion d'informations
 - Livre : IPv6, théorie et pratique
(O'Reilly ed. 03/1998, 2 ème édition 06/1999)
 - <http://www.urec.cnrs.fr/ipv6/>
 - séminaires
 - mailing list :
 - ipv6@imag.fr

Charte du G6 (2)




- ⊗ Infrastructure de test (G6-bone)
 - interconnexion des plates-formes de test 'françaises'
 - Banc d'essai pour une infrastructure nationale
- ⊗ Branche française du 6bone
- ⊗ Participation aux réunions RIPE & IETF
 - RIPE IPv6 wg
 - IPng, NGtrans, ION et 6Bone working groups





CNRS/UREC
B
·
T
U
Y

Les Activités du Groupe



- ⊗ Réunions 4 à 5 fois par an sur un des sites de tests
- ⊗ partenariats avec des constructeurs :
 - Cisco (NDA)
 - Telebit
 - Digital
 - ...
- ⊗ G6 Recherche :
 - faire le point sur l'avancement de la standardisation
- ⊗ Toutes informations disponibles sur :
 - <http://phoebe.urec.fr/G6/>

Séminaire IPv6 ARS 12.03.1999 100

Conclusion



- ⊗ Le G6 est un groupe ouvert à tous ceux qui veulent partager de l'expérience acquise sur la mise en œuvre et la supervision du (des) protocoles IPv6 sur les équipements traditionnels
- ⊗ les évolutions en cours (dans le cadre de Renater 2) vont nous permettre de commencer à expérimenter le trafic sur des liaisons natives (IPv6/ATM)
- ⊗ la phase « ultime » étant d'acheminer le trafic IPv6 comme le trafic IPv4 actuel -sans distinction- sur les réseaux de nos communautés.

IPv6

Bibliographie



- ⊗ IPv6, Théorie et Pratique. O'Reilly ed. (03/1998)
- ⊗ <http://www.urec.cnrs.fr/ipv6/Biblio.html>
- ⊗ <http://phoebe.urec.fr/G6/>
- ⊗ <http://www.ipv6.imag.fr>
- ⊗ <http://playground.sun.com/pub/ipng/html/ipng-main.html>
<http://playground.sun.com/pub/ipng/html/ipng-implementations.html>
- ⊗ <http://www.6bone.net>
- ⊗ mailing lists :
 - ipv6@imag.fr