www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Internet Protocol version 6

Plan

- Le Protocole IP
- Pourquoi un nouveau Protocole IP ?
- Caractéristiques et fonctionnalités du nouvel IP
- Structure des en-têtes IPv6
- Extensions d'en-têtes IPv6
  - fragmentation
  - sécurité ...
- Formats des adresses
- Les "nouveaux" protocoles associés à IPv6

Plan (2)

- Les Protocoles de routage
- Qualité de Service(s)
- IPv6 et ATM
- La mobilité
- Plan et techniques de Transition
- l'Internet version 6 : le 6bone, G6bone ...
- Bibliographie ...

Contributions à ce cours

Par ordre alphabétique ...

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

Internet Protocol: IP

- Protocole de niveau 3 de l'Internet
- IP est relativement simple, car dans l'Internet l'intelligence est aux extrémités (principe de bout en bout)
- IP est de type *best effort*
  - résiste facilement au facteur d'échelle
- IP fonctionne en mode non connecté
  - résiste aux pannes, aux attaques
- IP est ouvert, indépendant des systèmes; unificateur des différentes technologies de support physique
  - on a fait de l'IP sur des fils barbelés!

Pourquoi un nouveau Protocole IP ?

- *Actuellement la taille de l'Internet double tous les 12mois*
- *IP victime de son succès!*
- 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
  - un routage plus efficace

de IPv4 à IPv6

- Pour résoudre ces problèmes : IP, nouvelle génération
  - 1992: début du processus à l'IETF
  - 1994: premières définitions de IPv6
  - 1995: premières implémentations de tests
  - 1996: création du 6Bone, réseau expérimental
  - 1997: premiers produits commerciaux
  - 1998: premiers déploiements
  - ...

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

IPv6 Quelques Caractéristiques

- Adresse plus longue : 128 bits (16 octets)
  - adressage de 340 x 10 e36 équipements (plusieurs milliers/m2)
  - adressage hiérarchique
  - une partie peut-être l'adresse MAC (IEEE802)
    => autoconfiguration
- 3 types d'adresses :
  - Unicast : identifie une machine
  - Multicast : identifie un groupe de machines
  - Anycast : identifie une machine parmi un groupe

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

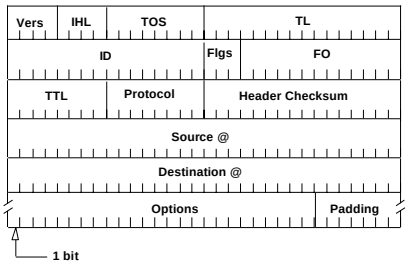
- Autoconfiguration : "*plug and play*"
  - Gestion de la mobilité
  - Renumérotation facile si changement de prestataire
  - Serveurs d'adresses (DHCP : *Dynamic Host Configuration Protocol)*
  - et SAA : *Stateless Address Autoconfiguration (RFC 1971)*
- Multipoint (*Multicast*) inclus de base
  - pour les routeurs et les clients
  - "scope" = meilleur routage des paquets multicast

=> plus besoin de Mbone ni de mrouted

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

IPv4 En-tête

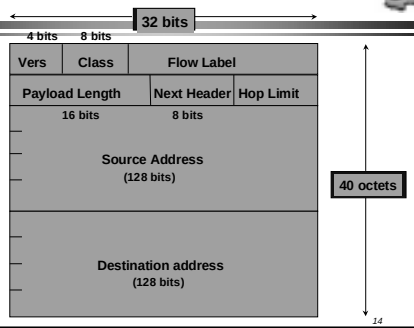


www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

IPv4 -> IPv6 changements de l'en-tête

- Header Length (IHL) : supprimé (en-tête de taille fixe)
- ToS --> Prio + 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 Checksum : supprimé
- Adresses : 32 --> 128 bits (4 --> 16 octets)
- Alignement 32 --> 64 bits

IPv6 En-tête



IPv6 les champs de l'en-tête

- Vers : Version Number (= 6)
- Priority :
  - champ *expérimental*, pris en compte par le routeurs intermédiaires, permettant à une source de caractériser son trafic.
- Flow label : identificateur de flots
  - numéro qu'utilise les routeurs pour référencer un contexte (au lieu d'utiliser les addr. IP + éventuellement les ports)
  - il existe 2 propositions pour le traitement de ce champ:
    - 1- la valeur du flow label reste inchangé tout au long du chemin
    - 2- les routeurs intermédiaires changent sa valeur (Tag Switching)
- Payload length : longueur du paquet après en-tête (en octets).

IPv6 les champs de l'en-tête *(2)*

- Next header : indique le type d'en-tête 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)**
- 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.

Des options d'IPv4 aux extensions d'en-têtes d'IPv6

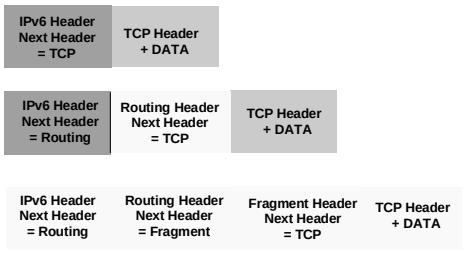
- Le champ *Option* d'IPv4 a essentiellement été défini à des fins de test ou de mise au point
- Il est peu utiliser pour les raisons suivantes:
  - la longueur du champ option est limité à 40 octets, ce qui limite l'emploi simultané de plusieurs options
  - il est forcément traité par ***tous*** les routeurs
  - son implémentation est souvent non-optimisée et ralentit considérablement le traitement des paquets par les routeurs
- Au lieu d'utiliser le concept d'options, IPv6 a défini le concept *d'extension d'en-tête* contenant plusieurs options

Des options d'IPv4 aux extensions d'en-têtes d'IPv6 (2)

- Une extension d'en-tête est soit traitée par tous les routeurs intermédiaires, quelques routeurs intermédiaires, ou par les destinations selon le type de l'extension
- 6 types d'extensions ont été définies pour l'instant; ils doivent être utilisées dans l'ordre suivant
  - Hop-by-Hop extension, Source Routing extension, Fragmentation extension, Authentification extension, Encryption extension, End-to-End extension

  (seul le Hop-by-Hop extension est traité par tous les routeurs; les routeurs ne traitent que l'en-tête IPv6 + le Hop-by-Hop extension)
- les extensions sont chaînées et situées entre l'en-têtes IPv6 et le payload (entête transport + les données)
- des fonctionnalités de bout en bout peuvent être rajoutées facilement

IPv6 en-têtes optionnelles



IPv6 les extensions d'en-têtes

- Hop-by-Hop Options Header :
  - transport d'information qui doit être examinée sur chaque noeud du chemin suivi par le datagramme IP.
  - exemple: option de *Router Alert* qui informe les routeurs que le paquet doit être complètement traité par le routeur avant d'être routé. Cette option est utilisée par RSVP.

en-tête suivant	lg. extension	type opt.	lg. option
			type opt.
lg. option			

  - 4 options sont définies pour l'instant...

IPv6 les extensions d'en-têtes (2)

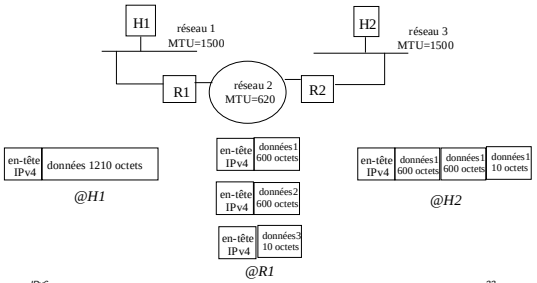
Prochaine ext	longueur	Routing=0	segments restants
reserved	bitmap strict/loose		
Addresse[0]			
...			
Addresse[N]			

- Source Routing Header :
  - routage à partir de la source
  - liste un ou plusieurs noeuds intermédiaires "à visiter" au cours de l'acheminement du datagramme
  - Le routage peut être strict (les routeurs de la liste doivent être voisins) ou libéral (loose)
  - Lorsqu'un routeur reçoit une paquet qui lui est adressé, il permute son adresse avec l'adresse du prochain routeur et remet le paquet vers cette adresse suivante

La fragmentation dans IPv6

- Dans IPv4, la fragmentation est réalisé par les routeurs
  - si un fragment se perd, le paquet est perdu
  - la fragmentation par les routeurs peut générer de très petits paquets (voir exemple précédent
- Dans IPv6, la fragmentation est évité si possible par le mécanisme de *MTU discovery*
- Si cette fragmentation est inévitable, elle est produite par la source ce qui évite l'émission de tout petit fragment

Rappel sur la fragmentation dans IPv4



IPv6 les extensions d'en-têtes (3)

- 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. Elle est déconseillée mais supportée pour certaines applications existantes qui suppose que la fragmentation existe

en-tête suivant	Réservé	place du fragment	0 0 M
identification			

  - bit M = 0 si dernier fragment sinon M = 1
  - identification permet de repérer les fragments d'un même paquet

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 { 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 pMTU = link MTU pour atteindre un voisin (first hop)
2. S'il y a un équipement intermédiaire dont link MTU < pMTU
   => destruction d'un paquet + émission d'un message ICMPv6 : "Packet size Too Large"
3. La source réduit le pMTU en utilisant l'information contenue dans le message ICMPv6

IPv6 les extensions d'en-têtes (4)

Les Extensions de Sécurité

- la sécurité est un des principaux objectifs de l'IAB
- Les fonctionnalités visées sont:
  - *l'authentification*: l'émetteur des données est bien celui qu'on croit
  - *l'intégrité*: les données ne sont pas altérées en chemin
  - *la confidentialité* : les données ne sont accessibles que pour les parties concernées.
- 2 extensions ont été définies:
  - l'extension d'authentification (AH: Authentification Header)
  - l'extension de confidentialité (ESP: Encryption Security Payload)
- ces extensions sont indépendantes des algorithmes de chiffrement utilisés
- administration des clés ne fait pas partie d'IPv6

IPv6 les extensions d'en-têtes (5)

- Authentification Header (AH)
  - L'authentification et intégrité est assurées par le même mécanisme: la somme de contrôle
    - l'émetteur et le récepteur partage un secret
    - l'émetteur calcule la somme de contrôle du paquet en émission, CRC, et le transmet dans l'en-tête d'extension AH (Authentification Header)
    - le récepteur fait la même opération sur les paquets qu'il reçoit et compare le résultat avec le CRC calculé par l'émetteur
      - si les deux résultats sont égaux alors :
        - le paquet est identifié car seul un émetteur connaissant la clé peut calculer la bonne valeur du CRC
        - le paquet n'a pas été corrompu sinon le résultat de la somme de contrôle aurait été faux (différent de celui émis par l'émetteur)

IPv6 les extensions d'en-têtes (6)

- Authentification Header (AH)

en-tête suivant	lg. extension	reservé
indice des paramètres de sécurité		
données d'authentification (nb variables de mots de 32 bits)		

- l'émetteur et le récepteur partagent une association de sécurité (algo., clés, durée de vie des clés), négociée lors de la procédure d'échange des clés et référencer par l'indice de paramètres de sécurité
- le champ données d'authentification contient le contrôle de somme calculé par l'émetteur
- différents algorithmes de calcul de sommes peut être utilisés mais MD5 est obligatoire

IPv6 les extensions d'en-têtes (7)

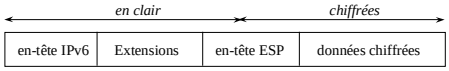
- Encryption (Privacy) Header ou Encapsulation Security Payload (ESP)
  - la confidentialité est assuré par chiffrage dans IPv6

  - 2 modes ont été définis:
    - mode transport: les informations du protocole de niveau supérieur + les données sont chiffrées
    - mode tunnel: le paquet entier est chiffré puis encapsulé
  - les algorithmes de chiffrement standard le DES (Data Encryption Standard) et le triple DES en mode CBC (Cipher Block Chaining).
  - d'autres protocoles peuvent être utilisés : IDEA, RC5

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

IPv6 les extensions d'en-têtes (8)

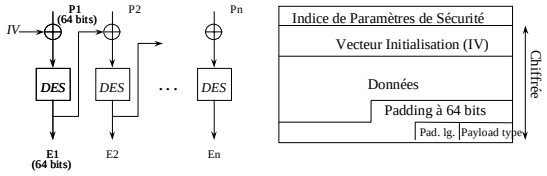
- ESP Header (2)
  - Seul le champ SPI (indice de paramètres de sécurité) est en clair dans l'en-tête ESP, le reste est chiffré.



  - le format de l'en-tête ESP dépend du protocole de chiffrage utilisé

IPv6 les extensions d'en-têtes (9)

- ESP Header : DES-CBC



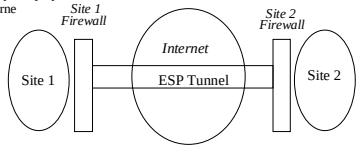
  - CBC (Cipher Block Chaining) évite les analyses de texte en clair connu (known plaintext) : l'attaquant connaît Pi et Ei.
  - IV varie d'un paquet à un autre

IPv6 les extensions d'en-têtes (10)

- La Gestion de l'association de sécurité
  - les mécanismes d'authentification et de confidentialité repose sur le partage d'une association de sécurité entre l'émetteur et le récepteur qui précise
    - le(s) algorithmes à utiliser
    - les clés
    - la durée de vie de l'association
  - différentes propositions existent, mais OAKLEY semble dominée
  - en absence d'une proposition officielle, on pourra toujours utiliser une distribution manuelle des clés

IPv6 les extensions d'en-têtes (11)

- Exemples d'utilisation d' IPv6 Sec
  - *les Intranets*
    - le mode tunnel peut être utilisé pour créer des tunnels sécurisés entre 2 firewalls de 2 sites distants et créer un *intranet*
    - le mode tunnel assure que l'entête IPv6 + extensions ne sont pas visibles; lorsque le paquet arrive au firewall destination, il est déchiffré et routé en interne



IPv6 les extensions d'en-têtes (12)

- Exemples d'utilisation d' IPv6 Sec
  - *les mobiles*
    - Mobile IP permet à une mobile de conserver sa connectivité tout en se déplaçant
    - Avec Mobile IP, un mobile fait toujours virtuellement partie de son réseau mère et peut donc accéder aux ressources locales
    - IPSec permet d'assurer l'authentification du mobile par son réseau mère et d'assurer l'intégrité et confidentialité des messages que le mobile et son réseau mère s'échange
  - *Les Protocoles de Routage*
    - la sécurité ne peut pas être assurée si les protocoles de routage ne le sont pas
    - les protocoles tel que RIP, OSPF ou IDRP, qui repose sur UDP/IP, peuvent bénéficier des mécanismes de IP Sec. pour authentifier et chiffrer les messages de mise à jour

IPv6 les extensions d'en-têtes (13)

- Sécurité au niveau des paquets IP
  - ne pas réinventer la roue à chaque application
  - les protocoles utilisés ont été testés et jugés suffisant
  - les implantations sont moins boggées (on peut l'espérer :-)
- Sécurité au niveau des paquets IP….pas toujours
  - dans certains cas, on doit utiliser dans mécanismes de sécurité
  - lorsque l'on ne fait pas confiance à l'OS
  - lorsque l'on veut utiliser des protocoles plus surs…quitte à payer plus cher...

IPv6 les extensions d'en-têtes (14)

- End-to-end Option Header (or Destination Option Header) :
  - transport d'information qui n'est à examiner que par le destinataire du datagramme.

en-tête suivant	lg. extension	type opt.	lg. option
			type opt.
lg. option			

  - 3 options sont actuellement définies dont celles de la mobilité...

Format des Adresses

- Adresse à usage local:
  - Adresse de lien
  - Adresse de site
- Adresse Globale
  - Adresse Compatible IPv4
  - Adresse mappée IPv4
  - Adresse standard (Aggrégée)
- Adresse Multicast
- Adresse Anycast

Format des Adresses

Adresse à usage Local : link local

10 bits	*54 bits*	*64 bits*
1111111010	000000 000	Interface ID

FE80::/64

- valable uniquement sur le lien local
- utilisée par le protocole d'autoconfiguration ND

Format des Adresses (2)

Adresse à usage Local : site local

10 bits	*38 bits*	*16bits*	*64 bits*
1111111011	00....00	Subnet ID	Interface ID

- adresse dont la validité est restreinte à un site
- utilisable, par exemple, pour site non connecté à l'Internet
- généralisation du concept d'adresses privées d'IPv4
- utilisable pour communication intra-site
- elle reste inchangée lors d'un changement de fournisseur de connectivité
- elle est définie par le préfixe FEC0::/48

Format des Adresses (3)

Adresse Compatible IPv4 :

000000 0000000	IPv4 Address
80 bits	*32 bits*

- Elle sert à 2 machines IPv6 de communiquer entre elles en IPv6 à travers un tunnel automatique IPv6/IPv4
  - un paquet transmis vers l'adresse ::a.b.c.d est encapsulé dans un paquet IPv4 vers l'adresse a.b.c.d
  - à destination, le paquet IPv6 est extrait et traité par IPv6

Format des Adresses (4)

Adresse "mapped" IPv4 :

000000 0000000	FFFF	IPv4 Address
80 bits	*16 bits*	*32 bits*

- permet à une machine IPv6 de communiquer en IPv4 avec une machine IPv4
- tout en restant dans la famille d'adresse AF_INET6
- utile pour écrire des serveurs IPv6 qui peuvent également répondre à des requêtes IPv4
  - en réception lorsqu'une requête IPv4 est recu, elle est traité par la pile IPv4 puis présentée aux applications sous la forme d'une requête IPv6 (par la couche socket)
  - en émission, la machine voyant une adresse IPv4 mappée, utilise la pile IPv4 pour envoyer des paquets IPv4

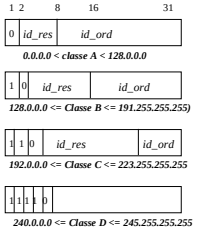
Format des adresses (5)

Adresse Multicast :

11111111	Flag	Scope	Group ID
8 bits	*4 bits*	*4 bits*	*112 bits*

Scope
1 : Node local
2 : Link local
5 : Site local
8 : Org. local
E : Global

Rappel IPv4 : les Adresses



- adresse IP : *<id_res, id_ord>*.
- 4 classes d'adresses sont définies:
  - *classe A*: 7 bits pour *id_res* (128 réseaux) et 24 bits pour *id_ord* (16777216 machines)
  - *classe B*: 14 bits pour *id_res* (16384 réseaux) et 16 bits pour *id_ord* (65536 machines)
  - *classe C*: 21 bits pour id_res (2097152 réseaux) et 8 bits pour les machines (256 machines)
  - *classe D*: adresse multicast

Leçons retenus d'IPv4

- Les adresses IPv6 doivent être plus longues car le nombre de machines connectés à l'Internet augmente
- Les adresses IPv6 doivent être distribuées avant une granularité plus fine que celle des 3 classes d'IPv4 qui produisent un gaspillage des adresses
- Les adresses IPv6 doivent être hiérarchiques afin de permettre une agrégation plus efficace et une réduction de la taille des tables de routage
- La hiérarchie des adresses doit tenir compte de la localisation géographique des sites afin d'optimiser les routes

Adresse globale IPv6

- 48 bits de topologie publique + 80 bits de topologie privée (site)

001	UAH	UAB*	UAS	Interface ID
3 bits	*13 bits*	*32 bits*	*16bits*	*64 bits*

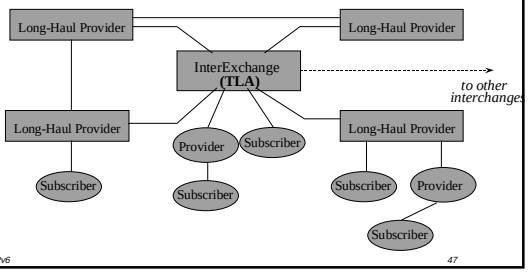
UAH : Unité d'agrégation haute (*TLA*)
Alloué aux différents points d'échange autour du monde.Le backbone ne doit maintenir qu'une entrée par point d'échange

UAB : Unité d'agrégation basse (*NLA*)
Alloué aux différents fournisseurs de service. L''UAB peut être divisé par chaque UAH comme bon lui semble (granularité + fine que classes d'IPv4).

001	UAH	UAB1	UAB2	Site	UAS	Interface ID

UA S : Unité d'agrégation de site (*SLA*)
Alloué aux différents sites pour organisation interne. Ce UAS reste identique même en cas de changement de fournisseur.

Plan d'adressage basé sur l'agrégation



Représentation des adresses

RFC 1884

- Format de Base (16 octets):
  - Adresse IPv6 Globale :
    - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- Format compressé :
  - FF01:0:0:0:0:0:0:43 => 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

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Nouveaux Protocoles

- Nouvelles fonctionalités spécifiées dans le protocole IPv6
- Autoconfiguration : Plug and Play
  - Configuration automatique
    - Stateless Address Autoconfiguration
    - DHCPv6 :Dynamic Host Configuration Protocol
  - Découverte des voisins (Neighbor Discovery, ND)
  - IPv6 facilite la configuration en réseau (exemple du dentiste)
- Path MTU discovery (pMTU)

Configuration automatique des adresses

- Traditionnellement la configuration d'une interface réseau est manuelle. Dans IPv6, elle est rendue automatique
- Cette phase d'autoconfiguration a pour objectifs:
  - l'acquisition d'une adresse quand une machine est attaché à un réseau pour la première fois,
  - l'obtention de la nouvelle adresse suite à la re-numerotaion du site
- Le processus d'autoconfiguration d'adresse IPv6 comprend
  - la création d'une adresse lien-local
  - la création d'une adresse unicast globale
  - la détermination de leur unificité
  - l'enregistrement de la nouvelle adresse auprès du DNS (en cours…)

Création de l'adresse lien-local

- A l'initialisation de son interface, la machine construit un identifiant sur 64 bits pour l'interface qui doit être unique au lien (souvent à partir de l'adresse MAC de l'interface)
- L'adresse lien-local est crée en concatenant le préfixe FE80::/10 à cet identifiant

- L'adresse ainsi constitué est encore interdite d'usage. Elle est dans un état provisoire car la machine doit encore vérifier l'unicité de cette adresse
- Si la machine détermine que cette adresse existe déjà, une intervention manuelle est nécessaire

Autoconfiguration à mémoire d'état (*stateful*)

- Autoconfiguration à mémoire d'état
  - DHCPv6 : *Dynamic Host Configuration Protocol*
    - s'appuie sur le protocole BOOTP (RFC 951)
    - et la version IPv4 de DHCP (RFC 1541)
  - 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)
  - Construire une adresse globale à partir de :
    - l 'adresse MAC de la machine
    - des annonces de préfixes faites sur le même câble *(par les routeurs)*

  => Ce mécanisme ne s'applique pas aux routeurs

Détection d 'adresse double

- Pour vérifier l 'unicité des adresses, l 'algorithme de DAD (Detection d 'Adresse Double) est utilisé.
- L 'algorithme consiste à:
  - envoyer un message de sollicitation avec comme adresse cible l'adresse provisoire
  - il y a alors 3 cas possible:
    - une machine répond; l 'adresse provisoire est utilisée comme adresse valide par une autre machine. L 'adresse provisoire ne peut être retenue
    - une machine répond; l 'adresse provisoire est également une adresse provisoire pour une autre machine. L 'autre ne peut être utilisée par aucune des machines.
    - Rien n 'est recu au bout d 'une seconde; l 'adresse provisoire est unique, elle passe de l 'état provisoire à celle de valide et est assignée à l 'interface.

Découverte des voisins (ND)

ND permet à un équipement de s'intégrer dans l 'environnement local, c.a.d il permet de dialoguer avec les équipements connectés au même support

Le protocole réalise les différentes fonctions:

- *Résolution d'adresses*: (idem ARP en IPv4)
- *Détection d'inaccessibilité des voisins*: permet d'effacer des tables de configuration les voisins devenus inaccessibles.
- *Configuration*
  - découverte des routeurs
  - découverte des préfixes (pour config. des adresses)
- *Découverte des paramètres* (MTU, nbre de sauts autorisé, si la configuration des adresses est sans ou avec état…)

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

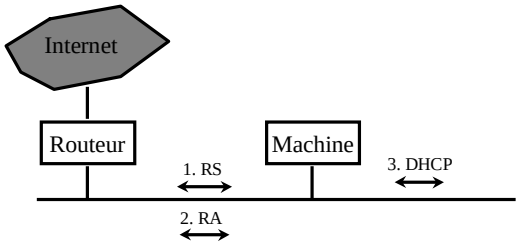
Découverte des voisins (2)

- ND spécifie 5 types de paquets ICMPv6 :
  - Router Solicitation (RS) :
    - un équipement requiert un RA tout de suite
    - émis à l'adresse multicast réservée aux routeurs sur le lien
  - 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
    - émis à l'adresse multicast réservé à toutes les machines du lien ou à l'adresse de la machine qui vient d'émettre un RS

Découverte des voisins *(3)*

- Neighbor Solicitation (NS) :
  - pour déterminer l'@ de niveau 2 d'un voisin
  - ou vérifier son accessibilité
  - également utilisé pour la DAD (Duplication Address Detection)
- 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

Auto-configuration



Qualité de Service

- Support pour la QoS : les paquets IPv6 contiennent un champ "priorité" et un champ "identifiant de flux"
  - Priorité:Utile pour la différentiation de services
  - Identifiant de flux: utilise pour identifier des flux de données (IP_Src, IP_Dest, Port_Src, Port_Dst) - Utilisé par IP switching, TAG switching, gestion de ressource (RSVP)...
- Toujours un problème ouvert :
  - mise en oeuvre dans les routeurs
  - correspondance avec les QoS sur ATM

IPv6 et ATM

On en est encore au stade d'élaboration des protocoles

- Les problèmes à résoudre:
  - Gestion du multicast (intégré au protocole IPv6)
    - Neighbor Discovery, Router Advertisement, Autoconfiguration
- Document de synthèse : RFC1932
  - présente les cinq modèles qui sont discutés dans les divers groupes de travail (IETF et ATM Forum):
    - Classical IP Model
    - NHRP Model
    - "Conventional" Model
    - Peer Model
    - PNNI and Integrated Model

La Mobilité Vue générale

La mobilité IPv6 s'appuie sur :

- L'expérience acquise dans IPv4
- Les nouvelles fonctionnalités d'IPv6 (les extensions d 'en-tête)
- 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 :

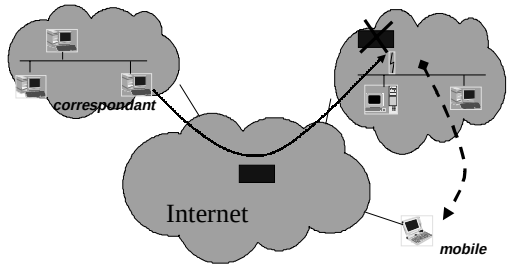
- vers le point d'attachement du mobile sur l'Internet
- vers l'adresse du mobile dans son sous-réseau mère

La Mobilité Problématique

- Dans l'Internet, une adresse IP
  - identifie un emplacement précis (un réseau + une machine)
  - identifie des connexions transport (TCP) ou applicatives..
- Lorsqu'un mobile change de point d'attachement réseau, il change forcément d'adresse IP.
- Si rien est fait, les paquets adressés à l'(ancienne) adresse du mobile seront perdus!
- Les objectifs du protocole Mobile IP sont:
  - maintenir la connectivité des mobiles
  - éviter la rupture des connexions lors des mouvements des mobiles

(Note: Mobilité # Réseaux Sans fil)

La mobilité Problèmatique (2)



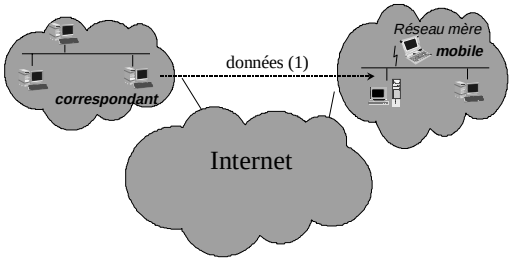
Mobile IPv6 Une vue globale

- Lorsqu'un mobile se déplace, il obtient une adresse temporaire par les mécanismes d'autoconfiguration de IPv6
- Il communique ensuite cette nouvelle adresse, par l'intermédaire d'un Binding Update, à son ***agent mére.*** L'agent mère d'un mobile est un routeur dans le sous-réseau mére du mobile.
- Lorsqu'un correspondant envoie un paquet au mobile pour la première fois, son agent mère intercepte le paquet et le redirige (en l'encapsulant) à l'adresse courante du mobile.
- Le mobile envoie également un BU à chacun de ses correspondants qui peuvent ensuite envoyer leurs paquets directement au mobile.

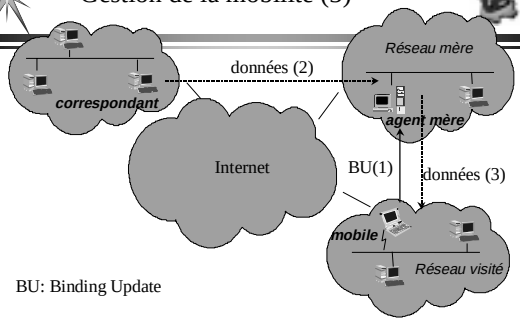
Les principales fonctionnalités de la Mobilité IPv6

- 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
- Un mobile:
  - est toujours *joignable* par son adresse mère
  - possède toujours une adresse temporaire lors de ces deplacements
  - détecte le changement de réseau à l'aide des mécanismes de ND

Gestion de la mobilité (2)

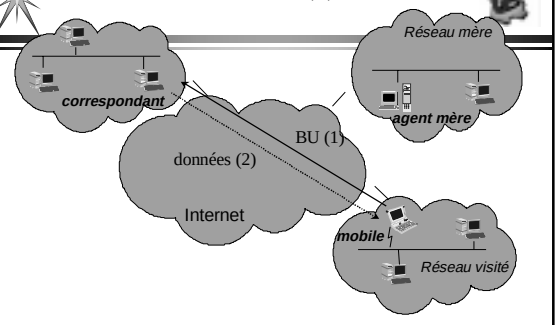


Gestion de la mobilité (3)

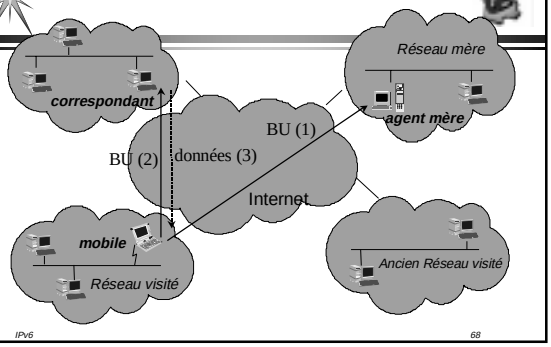


BU: Binding Update

Gestion de la mobilité (4)



Gestion de la mobilité (5)



Opérations du Mobile

- Un mobile envoie à chaque déplacement un Binding Update (BU)
  - à son HA et éventuellement à ces correspondants
  - Chaque BU inclut une durée de vie et sa nouvelle adresse temporaire (CoA)
  - Un mobile maintient une liste des correspondants à qui il a envoyé un BU
- Lorsqu'un mobile envoie des paquets, il peut soit:
  - utiliser son adresse mère comme adresse source
    - pas problème identification par les correspondants
    - mais problèmes possibles avec les firewalls (Ingress Filtering)
  - utiliser son adresse temporaire comme adresse source
    - pas de problèmes de firewalls
    - mais problème identification par correspondants =>Home Address Opt.
    - problème d 'anonymat (le mobile ne peut pas cacher sa localisation)
  - utiliser un tunnel bi-directionnel
    - les paquets sont tunnellés du mobile vers le HA, qui les décapsule et les envoie sur le réseau
    - l 'adresse source du paquet tunnellé est l 'adresse mère, celle du tunnel est l 'adresse temporaire.

Opérations du Correspondant

- Chaque correspondant maintient une liaison (Binding) par mobile
- Avant d'envoyer un paquet, le correspond examine sa table de binding
  - Si une entrée existe pour la destination
    - Le correspondant utilise un en-tête de Routage pour envoyer le paquet
    - l'adresse destination du paquet correspondant à l'adresse temporaire du mobile
    - l'adresse dans l'entête de routage est positionné à l'adresse mère du mobile
    - A destination, le mobile va automatiquement inverser ces 2 adresses…
  - Si il n'y a pas d'entrée correspondante, le paquet est envoyé directement à l'adresse destination.

Opérations de l'Agent Mère

- Lorsque le mobile est dans son réseau mère, l'agent mère est inactif
- Lorsqu'un mobile est en dehors de son réseau mère
  - l'agent mère intercepte les paquets adressés au mobile
  - et les tunnelle vers le mobile
    - l'entête de routage ne peut pas être utilisé dans ce cas, car il invaliderait l'entête d'authentification éventuel

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	ID lenght	Sequence Number
Lifetime (32)					
Care-of Address (128)					

  - Sequence : numérotation des BU + protection contre les «replay attacks»
  - Lifetime: Indique la durée de vie du BU
- tous paquets qui contient une option BU doit être authentifié

Option Binding Acknowledgement

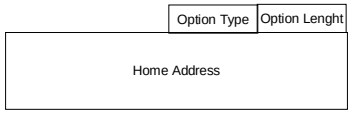
- Message d'acquittement basé également sur une extension d'en-tête Destination :

Option Type		
Option Length	Status	Sequence Number
Lifetime		
Refresh		

  - status: code indiquant si le BU a été accepté et sinon pourquoi
  - Lifetime: durée que le HA va garder ce BU
  - Refresh: ?
- Envoyé uniquement si le bit A est positionné dans le Binding Update envoyé par le mobile
- Doit également utiliser un *en-tête d'authentification*

Option Home Address

- Envoyé par le mobile, lorsqu'il utilise son adresse temporaire comme adresse source, comme identificateur.



- Home Address: l'adresse mère du mobile

Protocoles de routage

Transposition de ceux d'IPv4

- Protocoles intérieurs :
  - RIPng
  - OSPFng
- Protocoles extérieurs :
  - IDRP
  - BGP4+
  - BGP5

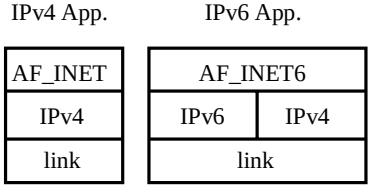
IPv6 Plan de Transition

- Philosophie générale :
  - Compatibilité de IPv6 avec IPv4 (postes de travail et routeurs)
    - conserver les @IPv4 déjà allouées
  - 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 !!!
  - Terminer la transition avant l'épuisement des @ IPv4

Méthodes de migration

- Applications
  - transparent (??) – ou adaptations simples (AF_INET -> AF_INET6)
  - une même application portée gère IPv6 et IPv4
- Couches réseau
  - machines à double pile
  - Tunnels configurés
  - Traduction d'en-têtes

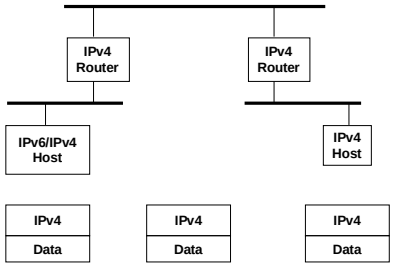
Applications



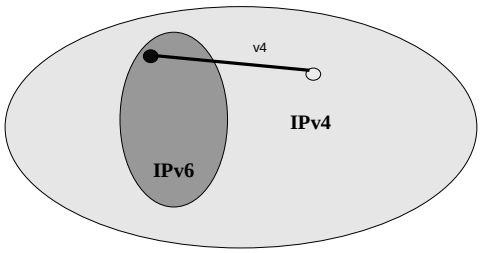
Couche Réseau transition (1)

- 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
  - les adresses mappées sont utilisées pour communiquer avec des machines uniquement IPv4

IPv6 Interopérabilité avec IPv4



Double pile: IPv6 – IPv4



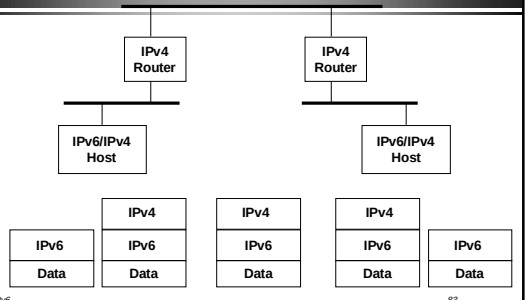
Couche Réseau transition (2)

- Encapsulation de IPv6 dans IPv4
  - encapsulation des paquets IPv6 dans des paquets IPv4

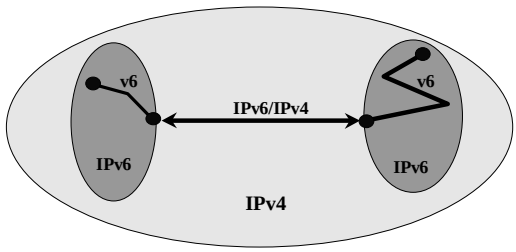
  => tunnels IPv6 à travers une infrastructure IPv4 :

  - tunnels configurés
  - tunnels automatiques

IPv6 Tunneling à travers IPv4



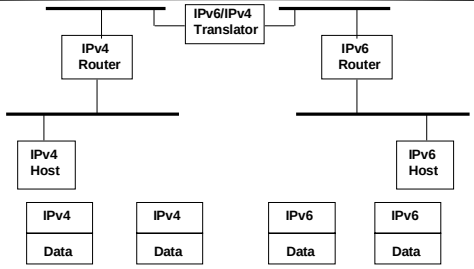
IPv6 – IPv6 à travers un tunnel IPv4



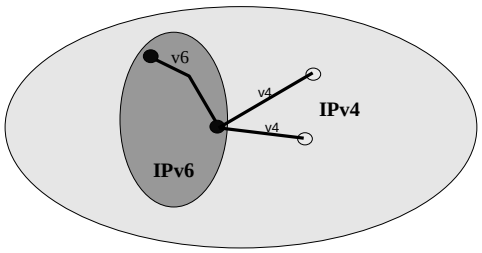
Couche réseau transition (3)

- Traduction des en-têtes IPv4 <--> IPv6
  - interopérabilité entre les équipements seulement IPv4 et les équipements seulement IPv6.
  - redevient très en vogue ... avec le NAT !

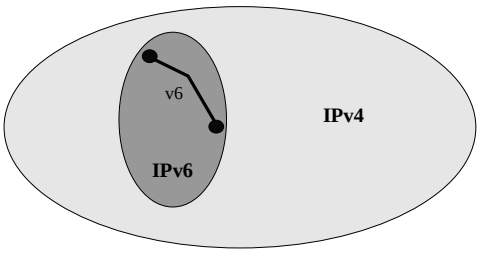
Traduction IPv6 <--> IPv4



Traduction d'en-tête IPv6 <–> IPv4



IPv6 – IPv6



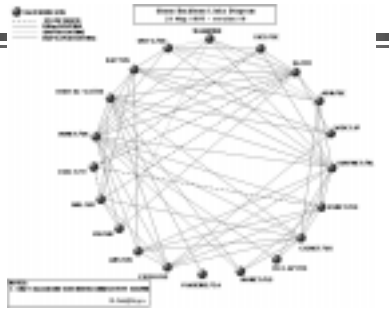
Le 6-bone et le G6

- 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: 130 sites & 27 pays
  - Groupe de travail IETF
  - http://www.6bone.net
- Le G6
  - Groupe français pour l'expérimentation de IPv6
  - Créé par l'IMAG et l'UREC(CNRS) fin 1995
  - Réunit académiques et industriels :
    IMAG, UREC, INRIA, ENST, Paris 7, Strasbourg,
    Institut Pasteur, Bull, Dassault electronique, Eurocontrol ...

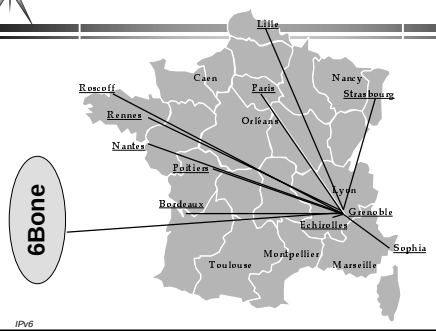
Carte du 6-bone (23/5/97)

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

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



Carte du G6-bone



IPv6 Groupes de travail

- Les groupes de travail de l'IETF :
  - ipng
  - ngtrans
  - 6bone
  - ion
- en Europe :
  - RIPE IPv6-wg
- en France :
  - G6

IPv6 Conclusions

- IPv6 est beaucoup plus qu'une révision d'IPv4; c'est un nouveau protocole.
- l'apport d'IPv6 est plus qu'un espace adressage plus important. IPv6 fournit également en natif des fonctionnalités très importantes pour les entreprises tel que l'auto-configuration, la sécurité, la gestion de la mobilité, le multicast, une meilleure agrégation des adresses…
- IPv6 est important pour les fournisseurs d'accès (agrégation des adresses, délégations plus souple des adresses), mais également pour les utilisateurs (nouveaux services tel que la sécurité, la mobilité.…)

IPv6 Conclusions

IPv6 …. Ce n 'est pas encore pour demain...

- IPv6 est un protocole très complexe et complet qui proposent de nombreux services difficiles à spécifier
- les concepteurs d'IPv6 veulent être sures de ne pas faire d'erreur et de développer le meilleur protocole possible à partir de l'expérience acquise avec IPv4
- IPv6 propose de mettre en œuvre des mécanismes, tel que la gestion des QoS, qui sont encore mal compris et sont du domaine de la recherche
- IPv6 est spécifier par un groupe de travail qui prend des décisions selon le principe de «Consensus et de codes qui tournent»
- la solution CIDR a retardé le problème causé par la pénurie des adresses IPv4; IPv6 n'est plus considéré comme une priorité

IPv6 Bibliographie

- http://www.urec.fr/IPv6/
- http://www.urec.fr/IPv6/G6.html
- http://www.ipv6.imag.fr
- http://playground.sun.com/pub/ipng/html/ipng-main.html

- mailing lists :
  - ipv6@imag.fr
  - ipng@urec.fr