

Réseaux

Protocole IPv6

Master Miage 1
Université de Nice - Sophia Antipolis

(Second semestre 2008-2009)

Jean -Pierre Lips (jean-pierre.lips@unice.fr)
(à partir du cours de Jean-Marie Munier)

Sources bibliographiques

- ✓ Cizault (G.) : IPv6 Théorie et pratique - 2ème édition - O'Reilly 1999
- ✓ Comer (D.E.) : Réseaux et Internet - CampusPress 2000
- ✓ Miller (M. A.): Implementing IPv6 - 2ème édition - M&T Books 2000
- ✓ Servin (C.) : Réseaux et Télécoms - 2ème édition - Dunod 2006
- ✓ Tanenbaum (A.S.) : Réseaux - 4ème édition - Pearson Education 2003

RFC :

- ◆ 1981 : Path MTU Discovery for IPv6
 - ◆ 2462 : Neighbor Discovery
 - ◆ 2640 : IPv6 Specifications
 - ◆ 2373 : IPv6 Addressing Architecture
 - ◆ 2463 : ICMPv6
 - ◆ 1933 : Transition Mechanisms for IPv6 Hosts and Routers
-
- ✓ Cours UREC du CNRS (www.urec.fr)

Principaux objectifs de IPv6

- Résoudre le problème de l'épuisement des adresses IPv4
- Réduire la taille des tables de routage
- Simplifier le protocole (en simplifiant l'en-tête IP) pour améliorer l'efficacité des routeurs
- Fournir plusieurs classes de service et permettre l'étiquetage des flux
- Fournir une meilleure sécurité (authentification et confidentialité)
- Gérer la mobilité des hôtes (autoconfiguration)
- Supporter les opérations de diffusion (*multicast*) de manière native (intégration du protocole IGMP dans ICMPv6)
- Permettre une coexistence souple avec IPv4

Limitations de l'adressage IPv4

- Nombre croissant de réseaux IP : 50000 réseaux dans 150 pays, en 1995, et 5 millions d'hôtes
- Adressage hiérarchique limité (réseau, sous-réseau, hôte) => entrée dans la table de routage pour chaque réseau à atteindre
- Capacité d'adressage (32 bits) :
 - théorique : 4.10^9
 - réelle : 2.10^8
- Épuisement des adresses IP, surtout de classe B (65% affectées, en 2002)
- Obtention possible d'adresses de classe C (40% affectées, en 2002), mais accroissement de la taille des tables de routage (inconvenient compensé par CIDR)

Adresses IPv6

- Adresses IPv6 définies sur 128 bits (16 octets)
- Capacité : $3 \cdot 10^{38}$ (soit $7 \cdot 10^{23}$ adresses par m² sur toute la Terre)
- Trois types d'adresses :
 - *unicast* : adresse individuelle (d'interface)
 - *multicast* : adresse de diffusion multidestinataire (à tout un groupe)
 - *anycast* : adresse de diffusion 'au premier vu' dans un groupe
- Note : plus d'adresses de diffusion générale (*broadcast*)
- Nouvelle notation (voir plus loin)
- Plan d'adressage agrégé (voir plus loin)

Notation des adresses IPv6

- Notation hexadécimale (groupes de 16 bits et ‘:’)
- Possibilités supplémentaires :
 - omission des zéros placés en tête
 - remplacement de groupes consécutifs de 16 zéros binaires par ‘::’
 - coexistence avec la notation IPv4
- Exemples :
 - ABCF:67B3:0000:0000:0000:34DE:0421:0012 *ou*
 - ABCF:67B3:0:0:0:34DE:421:12 *ou*
 - ABCF:67B3::34DE:421:12

 - 0:0:0:0:0:0:192.52.74.64 *ou*
 - ::192.52.74.64 *ou*
 - ::C034:4A40 adresse IPv4 compatible

 - 0:0:0:0:0:0:0:0 *ou* :: adresse indéterminée
 - 0:0:0:0:0:0:0:1 *ou* ::1 adresse de bouclage (\Leftrightarrow 127.0.0.1 en IPv4)

Préfixe d'adresse réseau IPv6

- Représentation des préfixes IPv6 similaire à la notation CIDR pour IPv4. Préfixe IPv6 :

adresse IPv6 / longueur du préfixe (nombre de bits)

- Exemples de représentation du préfixe de 60 bits

12AB00000000CD3 (hex) :

- ✓ 12AB:0000:0000:CD30:0000:0000:0000:0000 / 60
- ✓ 12AB::CD30:0:0:0:0 / 60
- ✓ 12AB:0:0:CD30:: / 60

- Combinaison d'une adresse d'hôte et d'un préfixe réseau.

Exemple :

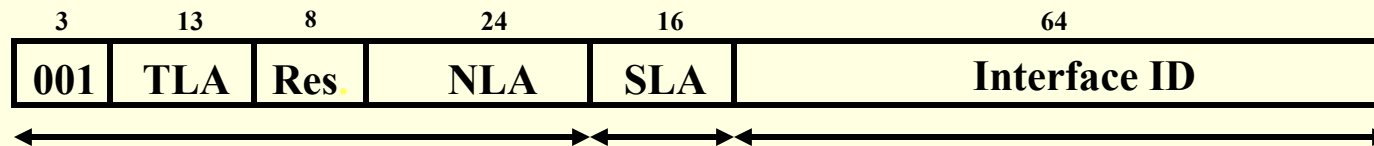
- ✓ adresse d'hôte : 12AB:0:0:CD31:2345:6789:ABCD:EF00
- ✓ adresse de réseau : 12AB:0:0:CD30:: / 60
- ✓ adresse combinée : 12AB:0:0:CD31:2345:6789:ABCD:EF00 / 60

Affectation des adresses IPv6

Préfixe (premiers bits)	Affectation	Fraction d'espace alloué
0000 0000	Réservé (compatibilité IPv4)	1 / 256
0000 0001	Non affecté	1 / 256
0000 001	Adresses NSAP OSI	1 / 128
0000 010	Adresses Novell Netware IPX	1 / 128
0000 011	Non affecté	1 / 128
0000 1	Non affecté	1 / 32
0001	Non affecté	1 / 16
001	Plan d'adressage agrégé	1 / 8
010	Non affecté	1 / 8
011	Non affecté	1 / 8
100	Non affecté	1 / 8
101	Non affecté	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 0	Non affecté	1 / 512
1111 1110 10	Adresses Lien-local	1 / 1024
1111 1110 11	Adresses Site-local	1 / 1024
1111 1111	Adresses multicast	1 / 256

Plan d'adressage agrégé

- Proposition de l'IETF (*Aggregatable Global Unicast Addresses*) RFC 2374
- Adressage hiérarchique à 3 niveaux :
 - topologie publique sur 48 bits :
 - ✓ 3 bits (001) identifiant le plan d'adressage
 - ✓ une unité d'agrégation haute (**TLA**, *Top Level Aggregator*) sur 13 bits
 - ✓ une partie réservé sur 8 bits
 - ✓ des unités d'agrégation basse (**NLA**, *Next Level Aggregator*), d'une taille totale de 24 bits
 - topologie de site (**SLA**, *Site Level Aggregator*) sur 16 bits
 - identificateur d'interface sur 64 bits, construit, par exemple, à partir de l'adresse MAC de l'interface

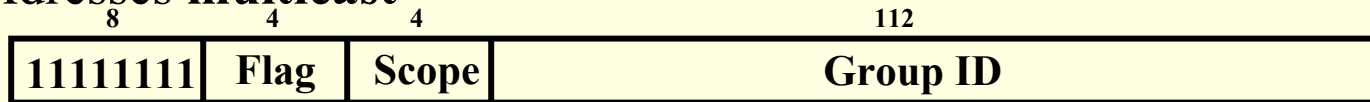


Autres adresses

- Adresses **anycast** : limitées (actuellement) à un routeur dans un sous-réseau



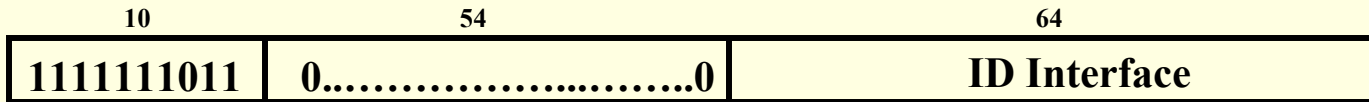
- Adresses **multicast**



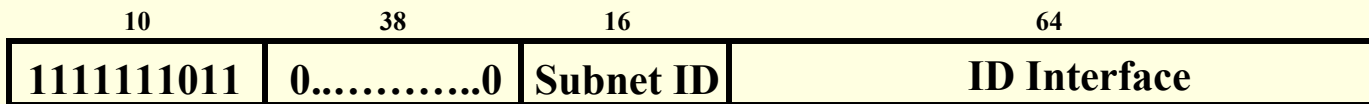
- Flag : 000T
 - ◆ T=0 : adresse multicast permanente (*well known*)
 - ◆ T=1 : adresse multicast temporaire
- Scope :
 - ◆ 1 : nœud (*node-local*)
 - ◆ 2 : lien (*link-local*)
 - ◆ 5 : site (*site-local*)
 - ◆ 8 : organisation (*organization-local*)
 - ◆ E : global

Autres adresses (suite)

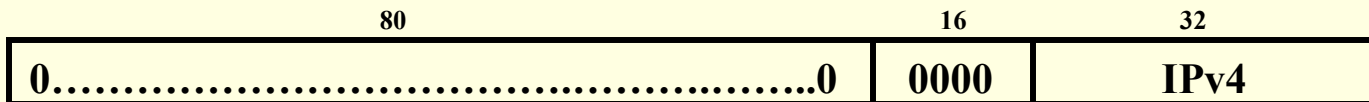
- Adresses lien-local



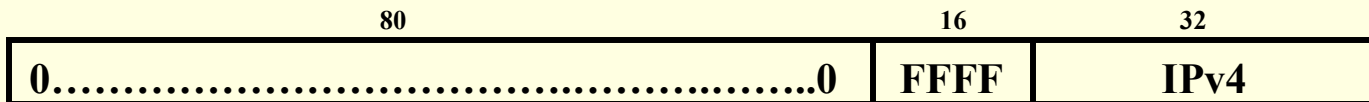
- Adresses site-local



- Adresses IPv4 compatibles



- Adresses IPv4 'mappées'



Simplification de l'en-tête IP

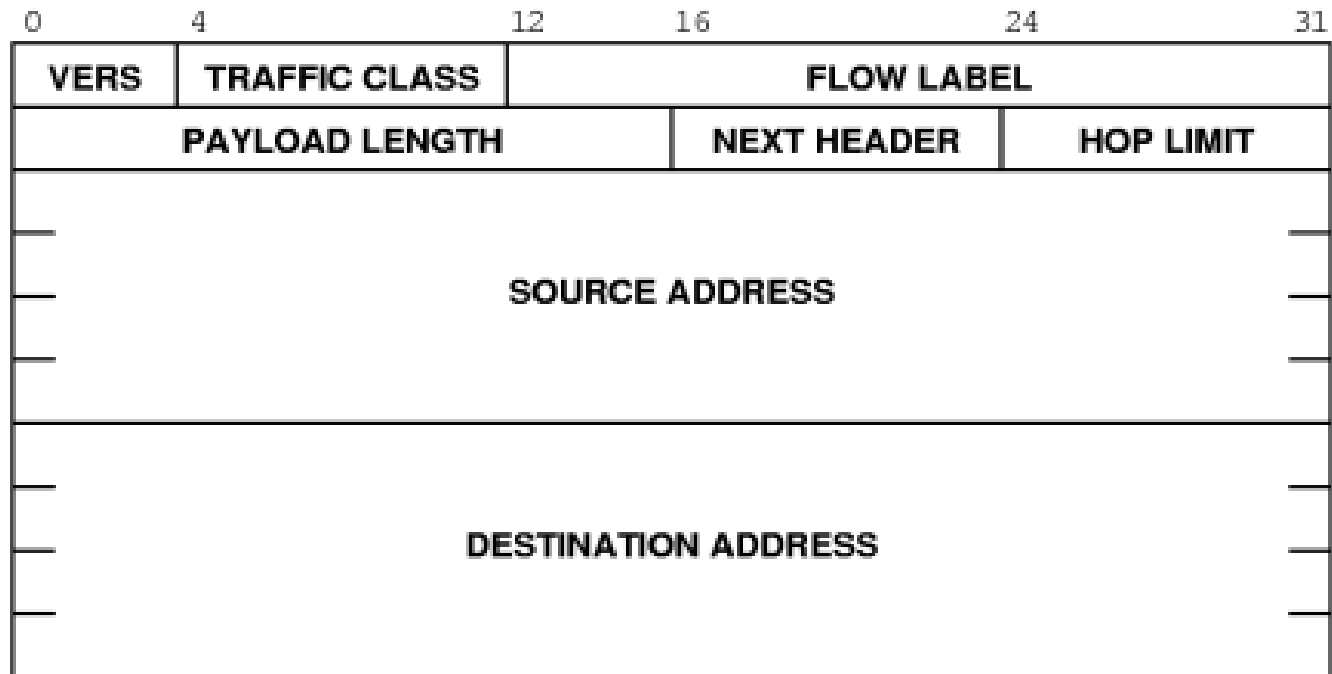
- En-tête IPv6 de taille fixe : 40 octets, en 5 mots de 64 bits
- Champ *Checksum* supprimé. Le total de contrôle de TCP/UDP, qui inclut un pseudo-en-tête, devient obligatoire avec UDP. De même, celui de ICMPv6 inclut le pseudo-en-tête.
- Options retirées de l'en-tête et remplacées par des en-têtes d'extension => routeurs plus performants
- Taille minimale des MTU = 1280 octets, et fonction de fragmentation retirée des routeurs. Fragmentation normalement superflue (découverte de la MTU de chemin, PMTU), sinon en-tête d'extension (exemple : NFS au-dessus de UDP)

En-tête IPv4 (rappel)

0	4	8	16	19	24	31
VERS	H. LEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		TYPE	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (MAY BE OMITTED)					PADDING	
BEGINNING OF DATA ⋮						

Source : D. E. Comer - Computer Networks and Internets - Prentice Hall 1999

En-tête IPv6



Source : D. E. Comer - Computer Networks and Internets - Prentice Hall 1999

Champs de l'en-tête IPv6

- **Version** (4 bits) : valeur = 6
- **Classe de trafic** (8 bits) : permet la différenciation des services
- **Identificateur de flux** (24 bits) : marquage de contexte
- **Longueur de charge utile** (16 bits) : taille du paquet, sans l'en-tête. Possibilité de paquets de taille > 65535 octets (Longueur = 0 et option Proche-en-proche)
- **En-tête suivant** (8 bits) : identification du prochain en-tête (similaire au champ Protocole de IPv4)
- **Nb_max_sauts** (8 bits) : -1 à chaque routeur traversé
- **Adresses** (2 x 128 bits)

En-têtes d'extension

- Possibilité d'adjoindre à l'en-tête de base des en-têtes d'extension, pour les options (adjonction récursive)
- A l'exception de l'option Proche-en-proche, les extensions ne sont pas prises en compte par les routeurs traversés

En-tête IPv6 Next Header = TCP	En-tête TCP + données
-----------------------------------	-----------------------

En-tête IPv6 Next Header = Routing	En-tête de routage Next Header = TCP	En-tête TCP + données
--	---	-----------------------

En-tête IPv6 Next Header = Routing	En-tête de routage Next Header = Fragment	En-tête de fragmentation Next Header = TCP	En-tête TCP + données
--	---	--	-----------------------

Source : RFC 2460

Extensions IPv6

- Format des en-têtes d'extension :
 - en-tête suivant
 - longueur d'en-tête
 - options : encodées type-longueur-valeur (TLV)
- Extensions possibles :
 - Proche-en-proche (*hop-by-hop*) : contenu examiné à chaque nœud (*jumbogrammes, Router Alert*)
 - Destination : contenu à examiner par la destination (ex : tunnel)
 - Routage : routage par la source
 - Fragmentation : effectuée par la source si taille > PMTU
 - Authentification : authentification et intégrité des données
 - Sécurité : chiffrement des données à protéger

Structure des messages ICMPv6

- **Type** (1 octet) : nature du message ICMPv6
 - 0 -127 : messages d'erreur
 - 128 - 255 : messages d'information
- **Code** (1 octet) : cause du message ICMPv6
- **Autres champs** (4 octets), selon la valeur du champ Type :
MTU, numéro de séquence, pointeur, identificateur...
- **Total de contrôle** (2 octets) : protection du contenu du message ICMPv6 et du pseudo-en-tête IPv6
- **Données ICMP** :
 - données (Echo), adresse, préfixe...
 - paquet qui a provoqué l'erreur

Messages d'erreur ICMPv6

Type	Signification
1	Destination inaccessible <ul style="list-style-type: none">aucune route vers la destination (code=0)communication administrativement interdite (code=1)a destination n'est pas un voisin (code=2)adresse inaccessible (code=3)numéro de port inaccessible (code=4)
2	Paquet trop grand
3	Temps dépassé <ul style="list-style-type: none">limite du nombre de sauts atteinte (code=0)temps de réassemblage dépassé (code=1)
4	Erreur de paramètre <ul style="list-style-type: none">champ d'en-tête erroné (code=0)champ d'en-tête suivant non reconnu (code=1)option IPv6 non reconnue (code=2)

Messages d'information ICMPv6

Type	Signification
128	Demande d'écho
129	Réponse d'écho
130	Demande de gestion de groupe multicast
131	Rapport de gestion de groupe multicast
132	Réduction d'un groupe multicast
133	Sollicitation de routeur (RS, <i>Router Solicitation</i>)
134	Annonce du de routeur (RA, <i>Router Advertisement</i>)
135	Sollicitation d'un voisin (NS, <i>Neighbor Solicitation</i>)
136	Annonce d'un voisin (NA, <i>Neighbor Advertisement</i>)
137	Redirection

Découverte des voisins

- Protocole *Neighbor Discovery (ND)* : RFC 2461
- Permet à un équipement de s'intégrer dans son environnement local
- Synthèse de ARP, ICMP Router Discovery, ICMP Redirect (entre autres), et ajout d'autres fonctions
- Fonctions :
 - ✓ résolution d'adresses
 - ✓ découverte des routeurs
 - ✓ découverte des préfixes
 - ✓ autoconfiguration des adresses
 - ✓ découverte des paramètres (MTU de lien, Nbr_max_sauts)
 - ✓ détection des adresses dupliquées
 - ✓ redirection
 - ✓ détection d'inaccessibilité des voisins

Découverte des voisins (suite)

- 5 types de paquets ICMPv6 pour ND
 - Sollicitation de routeur (RS)
 - ✓ émis par un équipement au démarrage pour obtenir des informations du routeur
 - ✓ message normalement émis à l'adresse multicast **FF02::2** (tous les routeurs d'un lien)
 - Annonce de routeur (RA)
 - ✓ émis périodiquement par les routeurs, ou en réponse à RS
 - ✓ donne la liste des préfixes, le nombre maximum de sauts, la MTU de lien...
 - Sollicitation de voisin (NS)
 - ✓ pour déterminer l'adresse physique d'un voisin ou vérifier qu'il est accessible
 - ✓ sert aussi pour la détection d'adresses dupliquées
 - Annonce de voisin (NA)
 - ✓ en réponse à NS ou pour propager une information (changement d'adresse)
 - Redirection

Configuration automatique

- Processus d'autoconfiguration d'adresse IPv6
 - création d'une adresse lien-local
 - vérification d'unicité
 - détermination de l'adresse unicast globale
- Deux méthodes d'autoconfiguration pour l'adresse unicast globale
 - autoconfiguration sans état (*stateless*) : génération de l'adresse à partir de l'identifiant d'interface et des annonces de préfixes faites par les routeurs sur le même lien
 - autoconfiguration avec état (*stateful*) : adresse fournie par un serveur ou un relais DHCPv6

Découverte de PMTU

- **PMTU** : *Path Maximum Transmission Unit*
- PMTU = valeur minimale des MTU de lien (linkMTU) sur un chemin donné (rappel : linkMTU min = 1280 octets)
- Découverte automatique de PMTU
 - l'émetteur fait l'hypothèse que $PMTU = linkMTU$
 - s'il y a un lien intermédiaire dont $linkMTU < PMTU$, le routeur associé détruit le paquet et renvoie un message ICMPv6 **Paquet trop grand**, qui contient la MTU acceptée
 - l'émetteur réduit la PMTU et recommence
- Utilisation de la PMTU
 - avec TCP : segmentation des données d'application
 - avec UDP : segmentation nécessaire par l'application, sinon fragmentation par IPv6 émetteur

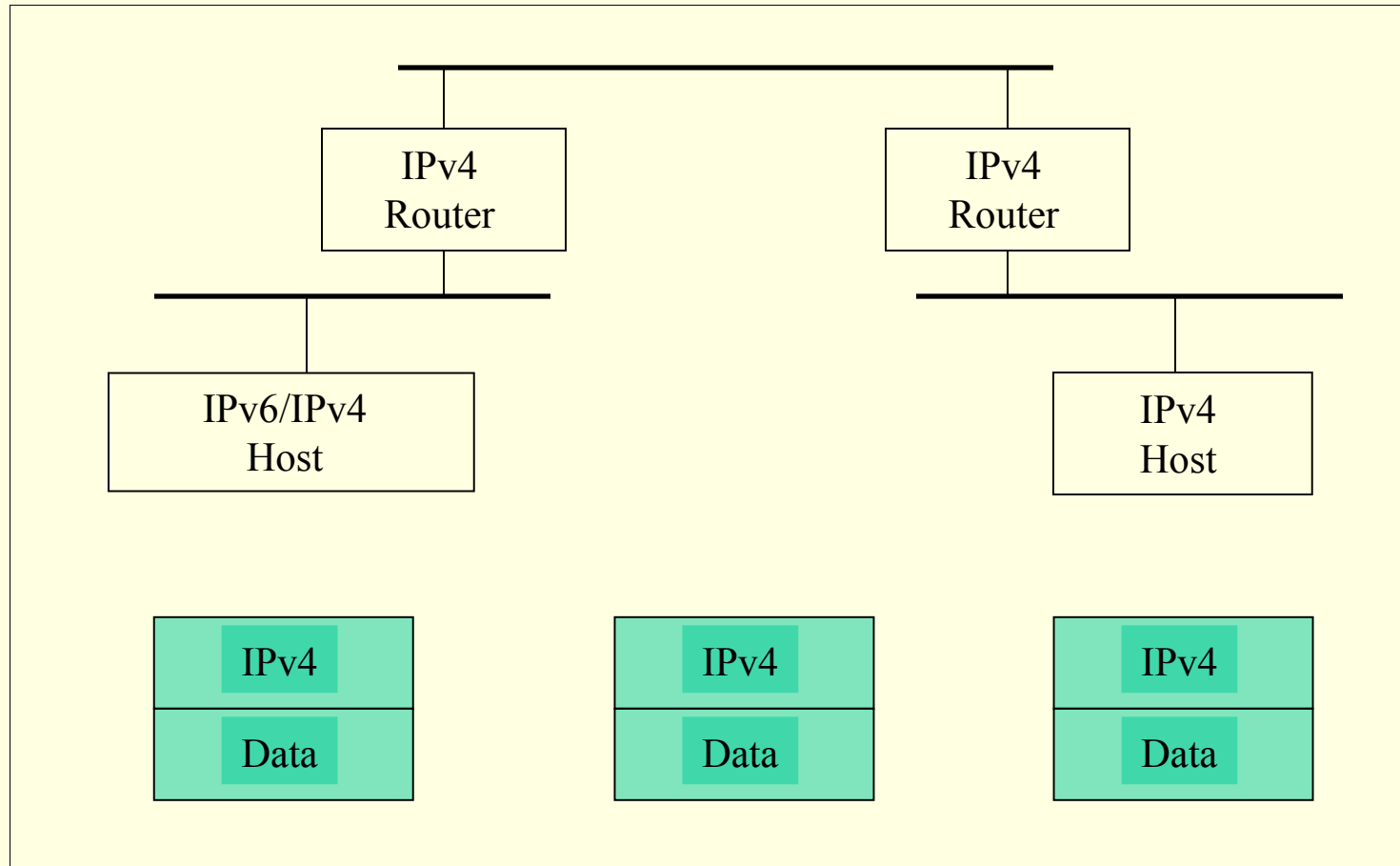
Classes de trafic

- Octet d'en-tête IPv6 permettant la différenciation des services (**DiffServ**, *Differentiated Services*)
- Deux classes :
 - trafic élastique
 - ✓ transfert des fichiers, courrier électronique, accès aux terminaux distants...
 - ✓ trafic tolérant au retard et à ses variations
 - trafic temps réel
 - ✓ applications audio et vidéo
 - ✓ grande sensibilité au retard et exigence de stabilité des retards
- Trois niveaux de service, selon niveau de priorité :
 - *Premium Service* (retard stable et faible)
 - *Assured Service* (bande passante garantie)
 - *Best Effort Service* (transfert 'au mieux')

Transition IPv4 - IPv6

- Prévoir des méthodes de coexistence et de transition souples (pas de jour J pour le passage d'IPv4 à IPv6)
 - permettre la mise à jour des hôtes IPv4 existants
 - permettre l'installation de nouveaux hôtes ou routeurs IPv6
 - permettre l'accès en IPv4 aux applications IPv6 des hôtes IPv4 (adresses IPv4 mappées)
- Trois techniques de transition :
 - double pile logicielle IPv4/IPv6
 - encapsulation de IPv6 dans IPv4
 - ✓ tunnels configurés
 - ✓ tunnels automatiques (adresses IPv4 compatibles)
 - traduction des en-têtes par un **NAT** (*Network Address Translator*)

Interopérabilité avec IPv4

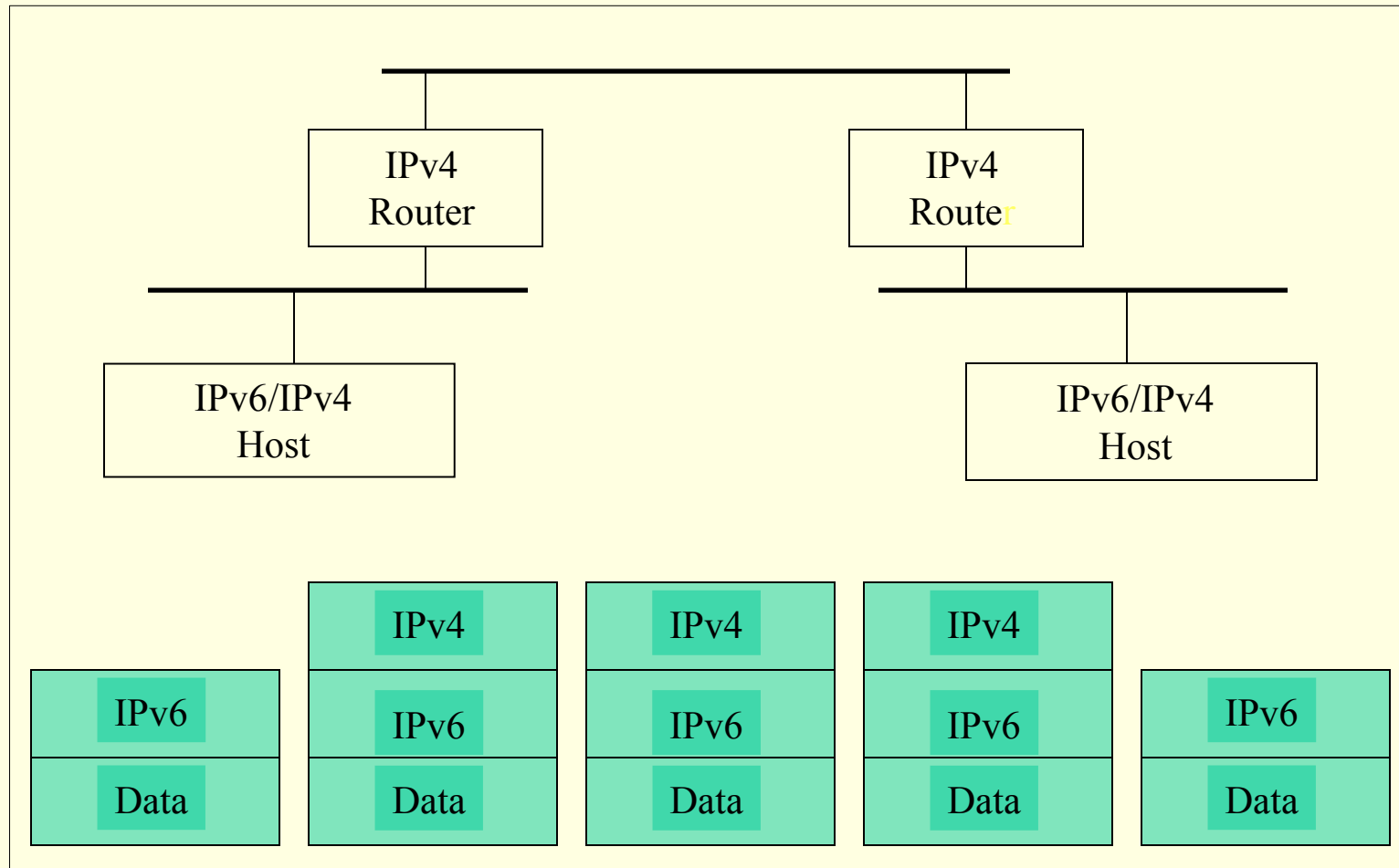


Source : Cours de l'UREC: IPv6

Tunnel à travers IPv4

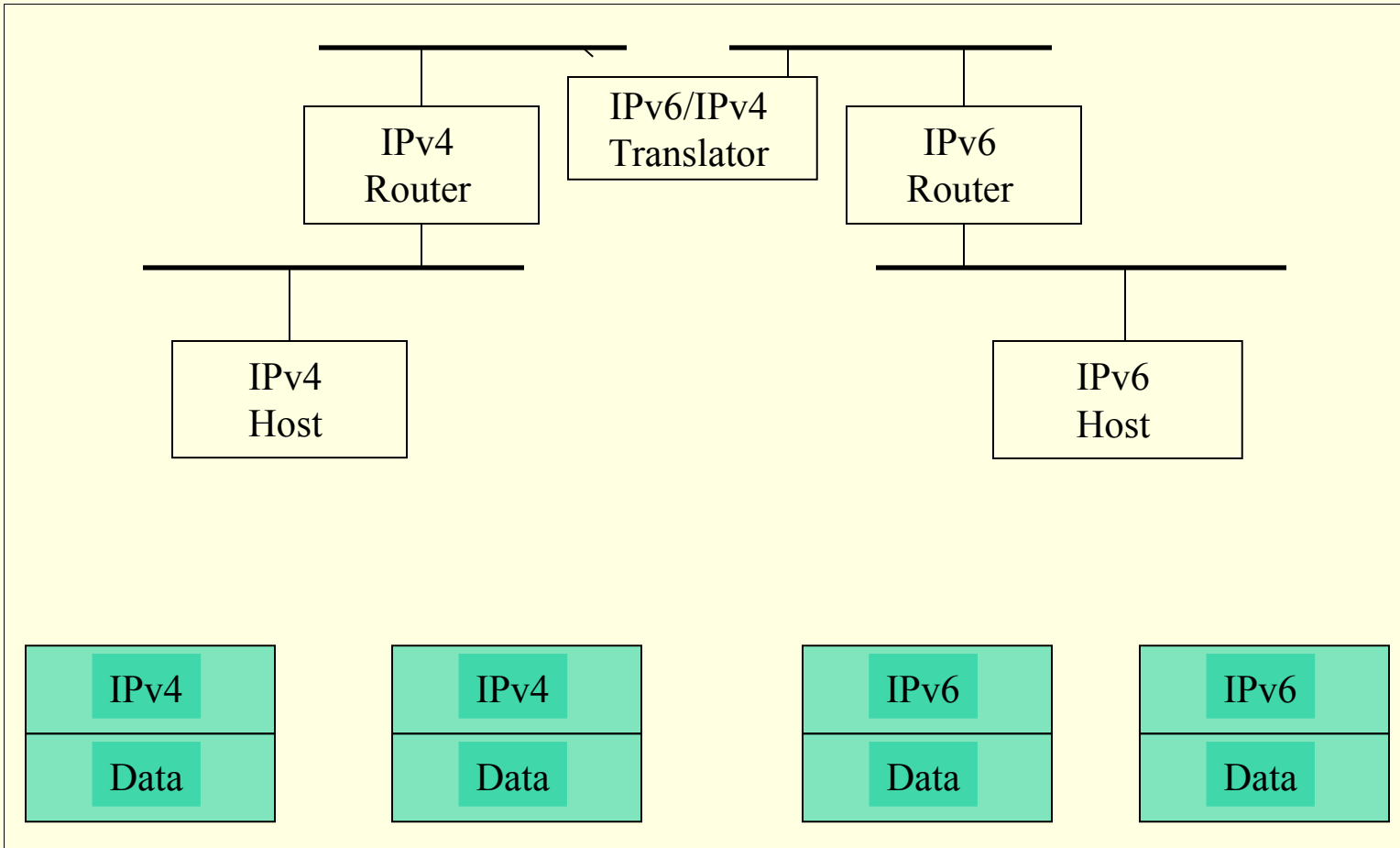
- Principe : encapsulation d'un datagramme IPv6 dans un datagramme IPv4 (champ 'Protocole' de IPv4 = 41)
- Deux types de tunnels :
 - tunnel configuré
 - ✓ liaison fixe entre deux machines (routeur-routeur ou hôte-routeur)
 - ✓ décapsulation par le routeur de terminaison du tunnel
 - tunnel automatique
 - ✓ accès d'une machine isolée à toutes les autres
 - ✓ tunnel routeur-hôte ou hôte-hôte
 - ✓ permet la réutilisation de l'infrastructure IPv4 (routeurs Ipv4)
 - ✓ utilisation d'adresses IPv4 compatibles
- Note : le principe du tunnel est généralisable : dans une phase avancée de transition, des systèmes IPv4 pourraient utiliser des tunnels IPv6

Tunnel à travers IPv4 (suite)



Source : Cours de l'UREC: IPv6

Traduction IPv6 \Leftrightarrow IPv4



Source : Cours de l'UREC: IPv6