

été capturé au cours d'une connexion FTP. Procéder au décodage de son ructure de l'en-tête IPv6 (voir cours).

fe 03 02 00 12 00 02

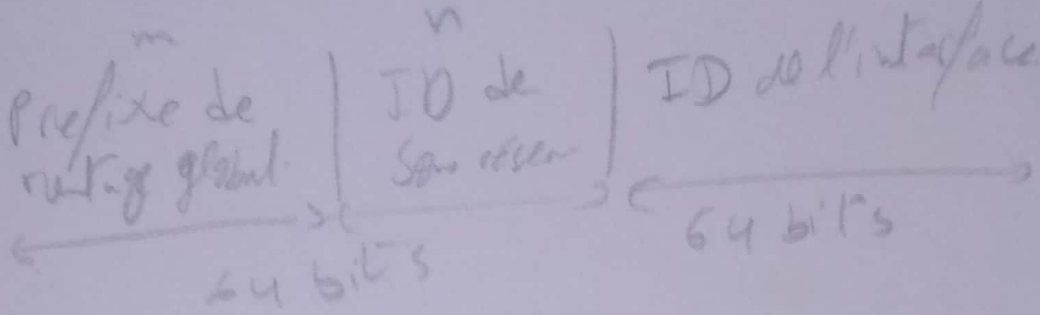
fe 03 05 10 02 00 01

2001:2b8:8ca3:0a

001202  
14+2

Adresse Unicast GUA:

54



0015  
001

- F → 15
- 10 → 16
- 11 → 17
- 12 → 18
- 13 → 19
- 14 → 20
- 15 → 21

LLA

10

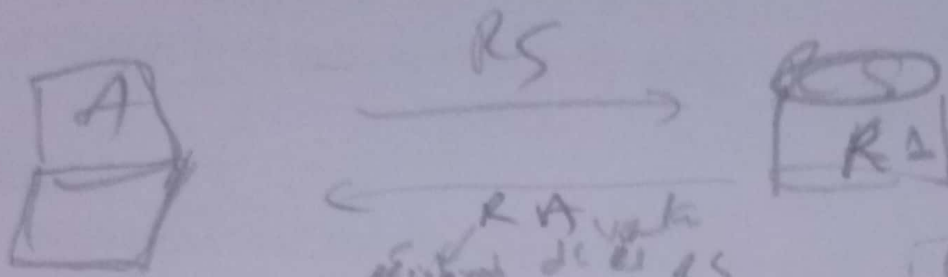
FE80::/10

FE10::1/10 LLA

FE 0000

FEF0::1

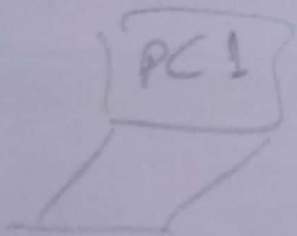




@ IPv6 LLA <sup>RS</sup> <sub>RS</sub> <sup>RA</sup> <sub>RA</sub>  
 @ Source: LLA-A  
 @ dest: FF02::2  
 Next Header: 58  
 Type: 133

@ Src: @ link R1  
 @ dest = PTV  
 Next H: 58 FF02::1  
 Type: 134  
 at site a  
 RS

(NS):



PC3, LLA: FE80::1 201: CAFE::1  
 @ multicast solicited: FF02::1: FF: FE::1

Type: 135 (NS) | Code

Connait IPV6 le PC ?  
 ? @ MAC de PC3



@ LLA: FE 80::202:CAFE:1  
 @ Multicast @ 50:FF02::1:FE:FE:4

@ Source MAC = @ MAC PC1  
 @ dest MAC = @ MAC: multicast  
 @ Source IPV6 = @ IPV6-PC1  
 @ dest: IPV6: @ multicast solicite de PC3  
 Type: 135(NS) | Code | Checksum  
 Target: @ IPV6: unicast à résoudre = NDP  
 @ MAC = @ MAC-PC1

@ MAC Source = @ MAC-PC3  
 @ MAC dest = @ MAC-PC4  
 @ Source IPV6 = @ IPV6-unicast-PC3  
 @ dest IPV6 = @ IPV6-unicast-PC4 (NS)  
 Type = 134(NA) | Code | Checksum  
 Target: @ IPV6 à résoudre  
 @ MAC: @ MAC recherché

## Travaux dirigés IPv6

### Exercice 1

- Donner une écriture en forme abrégée pour les adresses suivantes :
  - FEDC:0000:0000:0000:400:A987:6543:210F
  - 1FFF:0000:0A88:85A3:0000:0000:0C10:8001
  - FE80:0000:0000:0000:0000:0000:0000:0001
- Donner la forme abrégée de l'adresse suivante sachant que la longueur du préfixe est de 4 octets : 3EDC:BA98:7654:3210:0000:0000:0000:0000
- Quelle est la longueur d'un préfixe lien-local FE80:: ?
- Par quel type d'adresses IPv6 peut-on remplacer les adresses de diffusion IPv4?
- Donner le type de l'adresse IPv6 dans chaque cas :

Adresse	Type
2001:0db8:1:acad::fe55:6789:b210	@ GUA
::1	@ Link Local / @ Loop back
2033:db8:1:1:22:a33d:259a:21fe	@ GUA
FF00::db7:4322:a231:67c	@ Multicast (Groupe TD)
FF02::2	@ Multicast (tous les routeurs)
FE80::3201:cc01:65b1	@ LLA
FF02::1:FF24:CC52	@ Multicast sollicité

@ Unicast

### Exercice 2

- La carte réseau de votre PC a l'adresse MAC C5-23-12-A1-1B-88. Donner l'adresse lien local de cette interface en utilisant la méthode EUI-64.
- A partir de son adresse lien local IPv6, le PC rejoint son groupe multicast sollicité. Préciser l'adresse multicast sollicitée.
- Pour recevoir le trafic multicast, le PC doit ajouter une adresse MAC multicast à sa carte réseau. Préciser l'adresse MAC multicast.

### Exercice 3

- Comment un noeud recevant une trame Ethernet distingue si cette trame encapsule un paquet IPv4 ou IPv6 ?



3. Quelle est la longueur d'un préfixe lien-local FE80:: ?
4. Par quel type d'adresses IPv6 peut-on remplacer les adresses de diffusion IPv4?
5. Donner le type de l'adresse IPv6 dans chaque cas :

Adresse	Type
2001:0db8:1:acad::fe55:6789:b210	@ GUA
::1	@ Bnde local / @ loop back
2033:db8:1:1:22:a33d:259a:21fe	@ GUA
FF00::db7:4322:a231:67c → Groupe TD	@ Multicast
FF02::2	@ Multicast (tous les routeurs)
FE80::3201:cc01:65b1	@ LLA
FF02::1:FF24:CC52	@ Multicast sollicité

@ unicast

## Exercice 2

1. La carte réseau de votre PC a l'adresse MAC C5-23-12-A1-1B-88. Donner l'adresse lien local de cette interface en utilisant la méthode EUI-64.
2. A partir de son adresse lien local IPv6, le PC rejoint son groupe multicast sollicité. Préciser l'adresse multicast sollicitée.
3. Pour recevoir le trafic multicast, le PC doit ajouter une adresse MAC multicast à sa carte réseau. Préciser l'adresse MAC multicast.

## Exercice 3

## Correction TD IPv6

### Ex 1e

1) FEDC :: 400 : A987 : 6543 : 210F

· 1FFF : 0 : A88 : 85A3 :: C10 : 8001

· FE80 :: 1 LLA

2) 3EDC : BA98 : 7654 : 3210 : 0 : 0 : 0 : 0 → @ Réseau  
          ← préfixe                      SID

Réponse: La forme abrégée contenant juste le préfixe de notre adresse à savoir 3EDC : BA98 :: /32

3) FE80 :: /10

4) Multicast sollicité

### Exercice 2e

1) C5-23-12-A1-1B-88

· on génère l'ID de l'interface selon EUI-64.

Pour ce faire on divise l'@ MAC en 2 et on insère FFFE

C5-23-12-FF-FE-A1-1B-88

on inverse 7<sup>ème</sup> bit

⇒ on obtient ID-Interface: C7-23-12-FF-FE-A1-1B-88

⇒ Notre LLA est:

FE80 :: C723 : 12FF : FEA1 : 1B88

2) Notre @Multicast sollicite se compose de préfixe  
FF02::1: FF avec les 3 derniers q d'une @unicast.  
Ainsi notre PC rejoint le groupe Multicast dont  
l'@ est FF02::1: FFA1:1B88.

3) @Mac Multicast se compose de la façon suivante  
3333 + deux derniers hexet d'une @Multicast MAC.  
L'@Mac multicast est: 33-33-FFA1-1B88

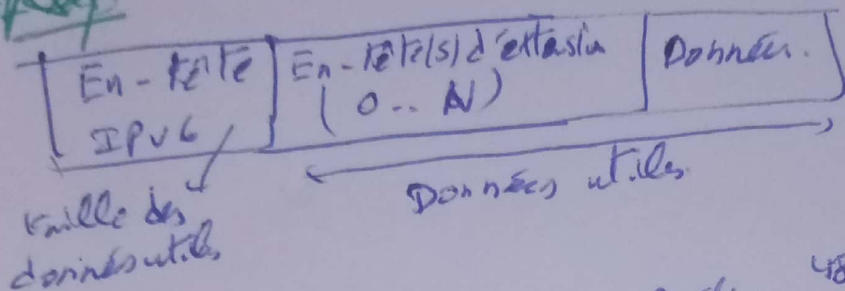
### Exercice 3e

- 1) Le Noeud examine le champ Type de la trame.  
$$\text{Type} = \begin{cases} (800)_{\text{hex}} \Rightarrow \text{le paquet à la version 4.} \\ (86DD)_{\text{hex}} \Rightarrow \text{le paquet à la version 6} \end{cases}$$
- 2) ①: version (4 bits) version 6 de l'IP.  
②: classe Traffic (8 bit)  
③: Etiquette de flux (20 bits)  
④: Taille des données utiles (16 bits): la taille du paquet  
et 400  
⑤: Entête suivant (8 bits) à la valeur 6  $\Rightarrow$  Notre paquet  
encapsule TCP.  
⑥: Hop limit (8 bits) (40)<sub>hex</sub> = (64)<sub>dec</sub>.  
Notre paquet peut parcourir 64 sauts au max.



- ⑦ @ IPv6 source (128 bits)
- ⑧ @ IPv6 destination (128 bits)
- ⑨ données  $\Rightarrow$  408 (taille des données)

Req.



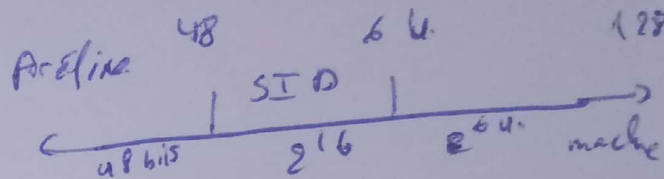
### Exercice 42

3) 2001:2:3::/48

$\Rightarrow$  on peut obtenir  $2^{16}$  sous-réseaux.  
 Dans chaque sous-réseau, on peut adresser  $2^{64}$  machines.

En tout, on pourra adresser  $2^{16} \times 2^{64}$  machines.

e) 2001:0660:2402:1001:208:EFF:FE DC:6A33/48



Le num. réseau est (2002)<sub>hex</sub> = (4097)<sub>dec</sub>

2001:0660:2402:1000:208:2FF:FE DC:9233/64

Le num. de num. sous-réseau et le dernier hexet et dans le préfixe sont (2000)<sub>hex</sub> = (4096)<sub>dec</sub>

2001:0665:2402:1001:1/32

Notre sous-réseau de le SID (2402:1002)<sub>hex</sub> = 98184097

4. Par quel type d'adresses IPv6 peut-on remplacer les adresses de diffusion IPv4?
5. Donner le type de l'adresse IPv6 dans chaque cas :

Adresse	Type
2001:0db8:1:acad::fe55:6789:b210	@ 6 u A
::1	@ Back Local / @ Loop Back
2033:db8:1:1:22:a33d:259a:21fe	@ 6 u A
FF00::db7:4322:a231:67c	@ Multicast
FF02::2	@ Multicast (1st les routers)
FE80::3201:cc01:65b1	@ LLA
FF02::1:FF24:CC52	@ Multicast sollicite

@ Unicast

### Exercice 2

1. La carte réseau de votre PC :

3) 2001:AC19:2:B:: / 64  
 → 2001:AC19:2:B::C8 / 64  
 2001:AC19:2:B::C8 / 64

adresse lien

licité. Préciser

st à sa carte

un paquet

### Questions

1. Un pa

signi

2. Pou

fea

# En-têtes d'extension IPv6

- Les options IPv6 sont remplacées par des en-têtes d'extension situés, dans un paquet, entre l'en-tête IPv6 et l'en-tête de la couche transport.
- Les en-têtes d'extension IPv6 actuellement définis sont :

• **Fragmentation** : Fragmentation et réassemblage. En IPv6, la fragmentation est effectuée uniquement par la source.

• **Routing** : utilisée par une source IPv6 pour spécifier des informations de routage telles que lister au moins un noeud intermédiaire.

• **Hop-by-Hop options** : utilisée pour spécifier des paramètres de livraison sur les nœuds intermédiaires.

• **Destination options** : Informations facultatives devant être vérifiées que par le nœud de destination (IP mobile)

• **Authentication** : Intégrité (vérifier que les données n'étaient pas modifiées), authentification (vérifier la source)

• **Encapsulating Security Payload** : Confidentialité des données

IPv6 Header  
Next Header = 6  
(TCP)

TCP Segment

IPv6 Header  
Next Header = 43  
(Routing)

Routing Header  
Next Header = 6  
(TCP)

TCP Segment

IPv6 Header  
Next Header = 43  
(Routing)

Routing Header  
Next Header = 44  
(Fragment)

Fragment Header  
Next Header = 6  
(TCP)

TCP Segment  
fragment

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	ICMPv5	58



# Adressage IPv6

- L'adressage proposé par IPv6 est l'apport le plus important car il vient corriger le plus gros défaut de IPv4 (nombre insuffisant d'adresses).
  - Comme avec IPv4, l'adresse IPv6 correspond à une interface (et non une machine).
  - Une interface peut avoir plusieurs adresses.
- Une adresse IPv6 est constituée de 128 bits (16 octets) contre 32 bits pour IPv4.
- L'écriture hexadécimale est utilisée pour IPv6 tels que chaque 2 octets sont séparés par deux-points :
- **Exemples:** <sup>hextet</sup>  
2001:0db8:0000:1111:0000:0000:0000:0200  
2001:0db8:0000:00a3:abcd:0000:0000:1234  
<sup>hextet</sup>
- Pour les adresses IPv6, **hextet** est le terme officiel qui désigne un segment de 16 bits=2 octets ou de quatre valeurs hexadécimales.
- Chaque adresse IPv6 contient 8 hextets.



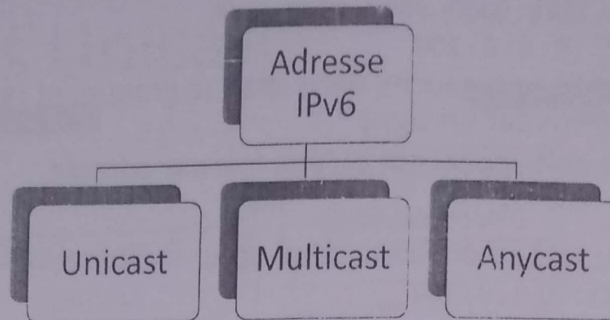
## Simplification de l'adresse IPv6

- La première règle pour réduire la notation des adresses IPv6 consiste à omettre les zéros (0) à droite. *Gauche*
- **Exemple**
  - 2001:0db8:0000:1111:0000:0000:0200
  - 2001:db8:0:1111:0:0:0:200
- On peut omettre les zéros à gauche dans chaque groupe, et remplacer une seule séquence de zéros par un signe "::".
- L'abréviation "::" ne doit apparaître qu'une fois par adresse.
- **Exemple**
  - 2001:0db8:0000:1111:0000:0000:0000:0200
  - 2001:db8:0:1111:0:0:0:200
  - 2001:db8:0:1111::200

## Préfixe IPv6

- La longueur du préfixe IPv6 est utilisée pour indiquer la partie réseau de l'adresse IPv6.
  - La notion de classe n'existe plus.
  - Les réseaux sont notés en utilisant la notation CIDR : Adresse IPv6 / Nombre de bits du préfixe réseau
  - La longueur du préfixe IPv6 recommandée pour les réseaux locaux et la plupart des autres types de réseaux est /64. *bit*
- **Exemple:**
  - Préfixe du réseau de l'adresse IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48
  - 48 bits situés complètement à gauche : 2001:db8:3c4d
  - Une représentation avec zéros compressés : 2001:db8:3c4d::/48 *Adresse réseau*
  - Le préfixe 2001:db8:85a3::/48 représente l'ensemble des adresses qui commence à 2001:db8:85a3:0:0:0:0:0 et finit à 2001:db8:85a3:ffff:ffff:ffff:ffff:ffff.

## Types d'adresses IPv6



*Unicast pas de broadcast en IPv6.*

## Types d'adresses IPv6

- Le protocole IPv6 a trois types d'adresses:

- **Unicast:** Cette adresse définit un hôte particulier. Un paquet émis avec cette adresse de destination n'est remis qu'à la machine ayant cette adresse IPv6.



- **Multicast:** Une adresse de type multicast désigne un ensemble d'interfaces. Les paquets envoyés à l'adresse multicast vont à tous les membres du groupe multicast.

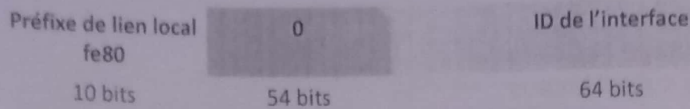


- **Anycast:** Anycast est un nouveau type d'adressage IPv6. Il identifie qu'un seul nœud, parmi un groupe de nœuds, reçoive l'information. Les paquets envoyés à l'adresse anycast vont au nœud membre du groupe anycast le plus proche de l'émetteur.



- Les adresses de type broadcast n'existent plus et sont remplacées par des adresses de type multicast prédéfinies.

- Chaque interface réseau compatible IPv6 doit avoir une LLA.
- Le préfixe d'une adresse de lien local est fe80::/10 (1111 1110 10 en binaire)
- Une adresse LLA a la structure suivante:



- Exemple d'une LLA: fe80::23a1:b152

*avant de changer:*

Exemple: si UL = 1 ⇒ @ Mac universelle (unique dans le monde)  
 si UL = 0 ⇒ @ Mac local (utilise dans les machines virtuelle)

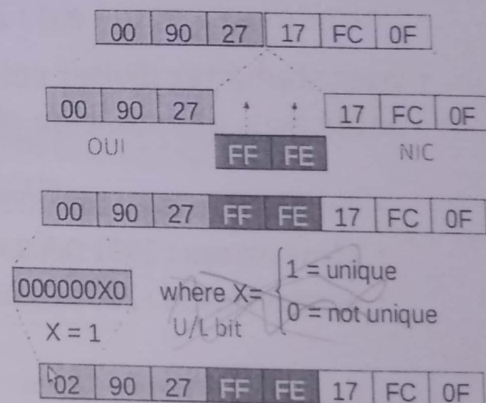
## ID de l'Interface

- Les deux types d'adresses global ou lien-local utilisent un identifiant sur 64 bits pour désigner une interface.
- Plusieurs techniques peuvent être utilisées pour définir l'ID de l'interface:

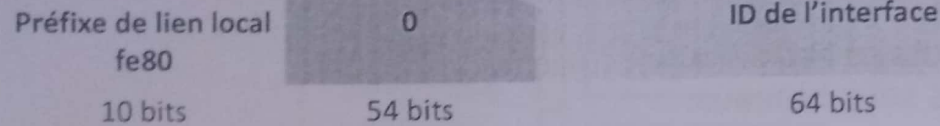
- **EUI-64** : Basée sur l'adresse MAC

1. On divise l'adresse MAC en deux parties de 24 bits:
  - Organizationally Unique Identifier (OUI)
  - Network Interface Controller (NIC)
2. On insère la valeur FFFE (en hexadécimal) au milieu de l'adresse MAC Ethernet 48 bits du client
3. On inverse le Universal/Local bit ( 7<sup>ème</sup> bit à gauche)

- **Aléatoirement** : 64 bits sont générées aléatoirement
  - pour des mesures de sécurité ⇒ Protéger l'adresse MAC



- Une adresse LLA a la structure suivante:



- Exemple d'une LLA: fe80::23a1:b152

*avant de changer:*

*Exemple: si UL = 1 => @ Mac universelle (unique dans le monde)  
si UL = 0 => @ Mac local (utilise dans les machines virtuelle)*

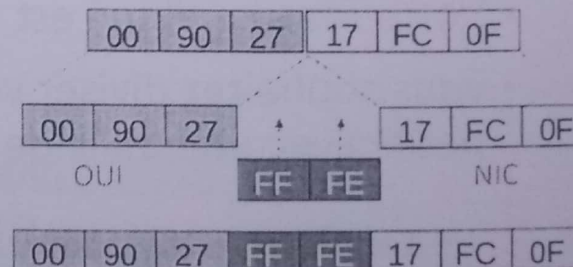
## ID de l'Interface

Les deux types d'adresses global ou lien-local utilisent un identifiant sur 64 bits pour désigner une interface.

Plusieurs techniques peuvent être utilisées pour définir l'ID de l'interface:

- **EUI-64** : Basée sur l'adresse MAC

1. On divise l'adresse MAC en deux parties de 24 bits:
  - Organizationally Unique Identifier (OUI)
  - Network Interface Controller (NIC)
2. On insère la valeur FFFE (en hexadécimal) au milieu de l'adresse MAC Ethernet 48 bits du client
3. On inverse le Universal/Local bit (7<sup>ème</sup> bit à gauche)



000000X0

X = 1

where X =  $\begin{cases} 1 = \text{unique} \\ 0 = \text{not unique} \end{cases}$   
U/L bit

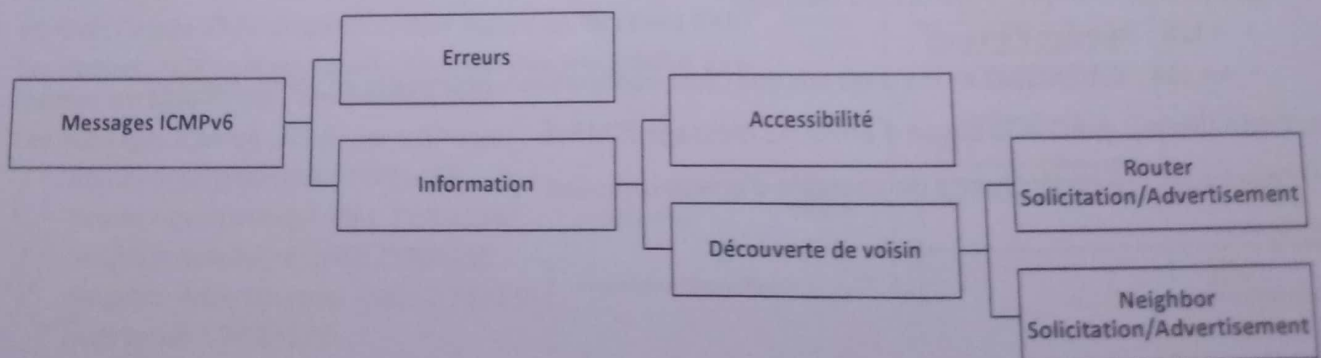


## Tableau Récapitulatif des adresses IPv6

Adresse non spécifiée	::
Adresse de loopback	0:0:0:0:0:0:1 ou ::1
Adresse unicast globale (GUA)	Actuellement attribuées 2000::/3
Adresse lien local (LLA)	fe80::/10
Adresse multicast	FF00::/8 FF02::1 : pour tous les nœuds FF02::2 : pour tous les routeurs
Adresse multicast sollicitée	ff02::1:ff00:0/104 avec les trois derniers octets d'une adresse unicast ou anycast

ICMP : signaler les erreurs

## ICMPv6



## Protocole ICMPv6

- ICMPv6 est un protocole plus générique que ICMPv4, utilisé pour :
  - rapporter des erreurs trouvées dans le traitement de paquets tout comme ICMPv4: Accessibilité de l'Hôte, Destination ou service inaccessible, Délai dépassé
  - effectuer des diagnostics
  - effectuer une découverte de voisinage
  - rapporter l'appartenance à un multicast

nouveau  
par IPv6

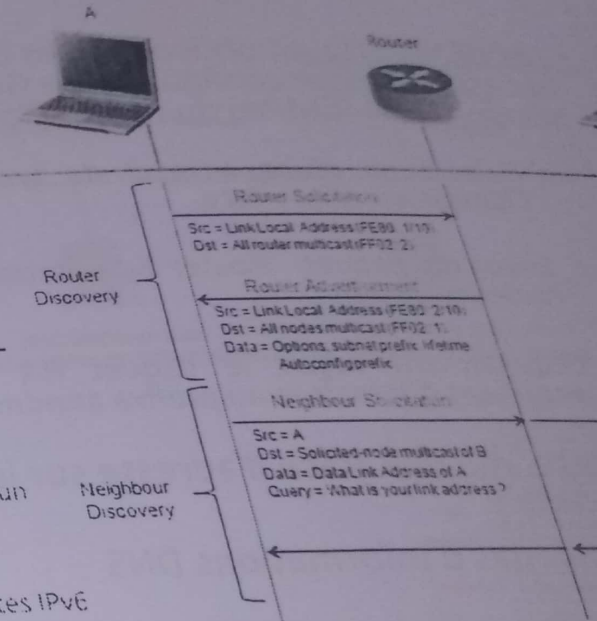
- Pour cette raison, les messages ICMPv6 sont catégorisés en deux types:
  - Message d'erreurs
  - Message d'information

## Format du paquet ICMPv6

# Messages d'information ICMPv6

- Messages d'accessibilité (ping)
  - Echo Request : TYPE=128
  - Echo Reply : TYPE=129
- Message de découverte de voisins IPv6
  - Le protocole Neighbor Discovery Protocol (NDP), RFC 4861, est utilisé dans IPv6 pour la découverte des voisins.
  - En IPv6, l'usage d'ARP disparaît et NDP assure les fonctions d'ARP
  - Les paquets NDP sont encapsulés dans des paquets ICMPv6 eux-mêmes encapsulés dans des en-têtes IPv6
  - Les messages ICMPv6 utilisés par NDP sont:
    - Router Solicitation (RS): TYPE=133
    - Router Advertisement (RA): TYPE=134
    - Neighbor Solicitation (NS): TYPE=135
    - Neighbor Advertisement (NA): TYPE=136
    - Redirection : TYPE=137

ate  
ndp  
et  
est  
ndp



## Généralités sur MLD

- Ce protocole est utilisé pour informer les routeurs présents sur un lien des hôtes en écoute, pour un groupe multicast donné, sur ce même lien.
- La version d'origine du protocole MLD (RFC 2710) (MLDv1) présente les mêmes fonctionnalités que le protocole IGMPv2 en IPv4.
  - Une des différences notables est que MLD s'appuie sur des messages ICMPv6 (alors qu'IGMP possède ses propres messages encapsulés en IP), ce qui justifie sa présence dans ce chapitre.
- Les messages MLD sont des messages ICMPv6 particuliers. Ils sont envoyés avec :
  - une adresse source IPv6 lien-local
  - le champ "nombre de sauts" fixé à 1
  - l'option "IPv6 Router Alert" activée => imposer aux routeurs d'examiner les messages MLD envoyés toutes des adresses multicast

⇒ Entête d'extention | Hop by Hop Options | ICMPv6 | MLD

| Router Alert = 1

Le contour doit être le contour de message



# Migration IPv4/IPv6

MLD: protocol multicast des IPv6

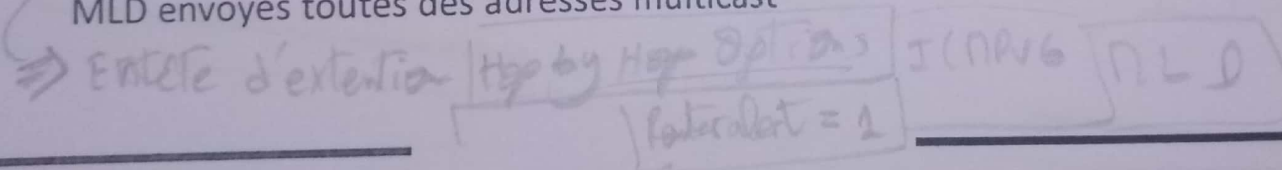
## Format du message MLD

Type	Code	Checksum
Maximum Response Delay		Reserved
Multicast Address		

- Type
  - Multicast Listener Query (Type = 130)
    - Interrogation générale: déterminer les adresses multicast qui sont sous écoute sur le lien local.
    - Interrogation spécifique: déterminer si une adresse multicast particulière est toujours sous écoute sur le lien local.
  - Multicast Listener Report (Type = 131)
  - Multicast Listener Done (Type = 132) *= quitter le groupe*
- Code, Reserved: initialisé à zéro et ignoré par le récepteur.
- Maximum Response Delay
  - Utilisé dans les messages d'interrogation (Multicast Listener Query).
  - Il spécifie le temps maximum autorisé avant l'envoi d'un rapport de réponse en millisecondes.
  - Dans tous les autres messages, il est mis à zéro par la source et ignoré par les destinataires
- Multicast Address
  - Pour les messages d'interrogation générale, ce champ contient la valeur 0
  - Pour les messages d'interrogation spécifique, ce champ est configuré sur l'adresse IP multicast du groupe sur lequel porte l'interrogation
  - Pour les messages de rapport d'adhésion et quitter groupe, ce champ contient l'adresse IP multicast du groupe reporté/quitté

## Généralités sur MLD

- Ce protocole est utilisé pour informer les routeurs présents sur un lien des hôtes en écoute, pour un groupe multicast donné, sur ce même lien.
- La version d'origine du protocole MLD (RFC 2710) (MLDv1) présente les mêmes fonctionnalités que le protocole IGMPv2 en IPv4.
  - Une des différences notables est que MLD s'appuie sur des messages ICMPv6 (alors qu'IGMP possède ses propres messages encapsulés en IP), ce qui justifie sa présence dans ce chapitre.
- Les messages MLD sont des messages ICMPv6 particuliers. Ils sont envoyés avec :
  - une adresse source IPv6 lien-local
  - le champ "nombre de sauts" fixé à 1
  - l'option "IPv6 Router Alert" activée => imposer aux routeurs d'examiner les messages MLD envoyés toutes des adresses multicast



Le routeur doit lire le contenu de message