Cours Réseaux - IPv6

Thierry Vaira

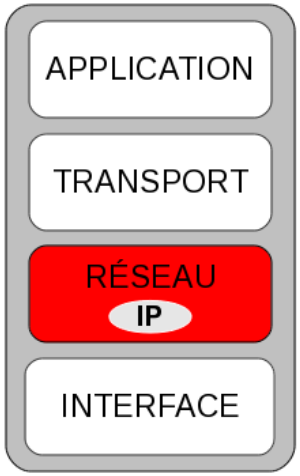
BTS SN-IR

tvaira@free.fr ☮ v0.1

Sommaire

Définition

- Rappel : de manière générale, les adresses forment une notion importante en communication et sont **un moyen d'identification**.
- Dans un réseau informatique, une **adresse IP** est **un identifiant unique attribué à chaque interface avec le réseau IP** et associé à une machine (routeur, ordinateur, etc.). C'est une adresse ***unicast*** utilisable comme adresse source ou comme destination.



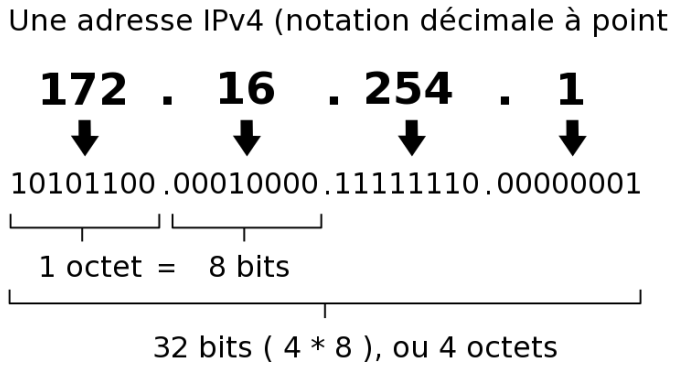
Modèle DoD

IP signifie *Internet Protocol*.

Différentes versions des adresses IP

Il existe deux versions pour les adresses IP :

- **version 4** : les adresses sont codées sur **32 bits**
  - Elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points.



- **version 6** : les adresses sont codées sur **128 bits**
  - Elle est généralement notée par groupes de 4 chiffres hexadécimaux séparés par ':' (exemple : FE80:0000:0000:0000:020C:76FF:FE21:1C3B).

`https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/lipv6/suivi-epuisement-adresses-ipv4.html`

Historique

En quelques dates :

- Septembre 1981 : Internet Protocol (IP)
- Octobre 1984 : Création du concept de sous-réseau (*Internet subnets*)
- Septembre 1993 : Abandon de l'adressage par classes et utilisation de CIDR (*Classless Inter-Domain Routing*)
- Février 1996 : Réservation d'adresses pour l'usage privé
- **Décembre 1998 : Spécification d'*Internet Protocol* Version 6 (IPv6)**
- **25 novembre 2019 : RIPE NCC a annoncé la pénurie d'IPv4 !**

Notation des adresses IPv6

La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une **écriture hexadécimale**, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points ' :' :

Exemple : La notation complète comprend exactement 39 caractères

2001:0db8:0000:85a3:0000:0000:ac1f:8001

Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :

2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points (::). Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en :

2001:db8:0:85a3::ac1f:8001

Excercice n°1

I. Donner une écriture en forme abrégée pour les adresses suivantes :

a) 2001:0001:0002:014E:F140:0102:8012:00AE
b) FEDC:0000:0000:0000:0400:A987:6543:210F
c) 1FFF:0000:0A88:85A3:0000:0000:0C10:8001
d) FE80:0000:0000:0000:0000:0000:0000:0001

II. Est-ce que les adresses suivantes sont des adresses IPv6 valides ?

a) 2001:14C8::871:206:A14:23
b) 2001:14C8::871:206::A14:23
c) 2001:14C8:0:0134::A120:E001
d) 200F:23G5:23:1:45:A234::1

III. Écrire sous la forme complète les adresses IPv6 suivantes :

a) 2001:14C8::871:206:A14:23
b) 2002:203::AEF:12:0:1B1:1
c) 2003::2
d) 2001::45:0:6

Type d'adresses IPv6

Les bits de poids fort (à gauche) d'une adresse IPv6 déterminent le type d'adresse. Ce champ de longueur variable est appelé « préfixe de format » ou simplement **préfixe** :

Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques (utiliser fd00::/8 sur un réseau local)
fe80::/10	Adresses locales lien
ff00::/8	Adresses multicast

En IPv6, il n'y a pas d'adresse de *broadcast*. Elle est remplacée par des adresses *multicast*.

Décomposition

Les adresses IPv6 sur **128 bits** sont décomposées en :

- un **préfixe** de localisation public : 48 bits
- un champ **sous-réseau** de topologie locale du site (subnet) : 16 bits
- un identifiant de l'**interface** (basé sur l'adresse MAC ou aléatoirement) qui garantie l'unicité de l'adresse (équivalent à *hostid*) : 64 bits

Structure des adresses unicast globales

champ	*préfixe*	*sous-réseau*	*interface*
bits	48	16	64

Structure des adresses link-local

champ	*préfixe*	*zéro*	*interface*
bits	10	54	64

1111111010

Format d'une adresse multicast

champ	*préfixe*	*drap.*	*scope*	*groupe*
bits	8	4	4	112

11111111

Structure des adresses locale unique

champ	*préfixe*	*L*	*ID globale*	*Subnet*	*Interface*
bits	7	1	40	16	64

1111110

Remarques IPv6

- Les adresses constituées entièrement de 0 ou de 1 ne jouent pas de rôle particulier en IPv6.
- Pour les cas où le ':' a un sens (par exemple dans une URL), on met l'adresse IPv6 entre `[]` pour éviter toute confusion. Exemple : `http://[::1]/`
- La notion historique de classes a totalement disparu, au profit de l'utilisation exclusive des préfixes et de la notation CIDR avec le *slash* / et le masque, déjà utilisés en IPv4. Les masques par défaut disparaissent aussi.
- En IPv6, les sous-réseaux ont une taille fixe de /64, c'est-à-dire que 64 des 128 bits de l'adresse IPv6 sont réservés pour les hôtes dans le sous-réseau.
- L'IANA alloue des blocs de taille /23 à /12 dans l'espace unicast global (2000::/3) aux cinq RIR. Les RIR les allouent aux LIR sous forme de blocs de taille minimale de /48.

Adresse IPv6 mappant IPv4

Une adresse IPv6 mappant une adresse IPv4 constitue un **cas spécial** d'adresse IPv6. Elles sont utilisées par la pile IP pour représenter des adresses IPv4 dans des applications IPv6 (mais ne doivent pas se trouver dans le réseau). Une telle adresse IPv6 a une notation ::`ffff`:0:0/96 et elle est constintuée de la manière suivante :

- les premiers 80 bits fixés à zéro,
- les 16 suivants à un et
- **les 32 bits restants représentent une adresse IPv4**.

Remarque : Exception spéciale à la notation des adresses IPv6, les adresses correspondant à de l'IPv4 sont communément représentées avec leurs 32 bits significatifs notés comme en IPv4.

Exemple : ::`ffff`:c0a8:3402 → ::`ffff`:192.168.52.2

Adresses obsolètes

Adresses IPv6 obsolètes

Préfixe	Description
3ffe::/16 5f00::/8	Adresses utilisées par le réseau expérimental 6bone
fec0::/10	Adresse locale de site
::a.b.c.d/96	Adresse compatible IPv4 (a.b.c.d est une adresse IPv4)

- Adresses locales de site : obsolètes depuis 2004 avec la RFC 3879 et remplacées par les adresses locales uniques avec la RFC 4193.
- Adresses compatibles IPv4 : obsolètes par la RFC 4291.

DNS (*Domain Name System*)

- Les noms d'hôtes sont associés à des adresses IPv6 grâce à l'enregistrement `AAAA` :
  `www.ipv6.ripe.net. IN AAAA 2001:610:240:22::c100:68b`
- L'enregistrement inverse `PTR` est réalisé sous ip6.arpa en inversant l'adresse écrite sous forme canonique :
  `...0.1.6.0.1.0.0.2.ip6.arpa. IN PTR www.ipv6.ripe.net.`

Excercice n°2

En fonction de leur préfixe, déterminer le type des adresses suivantes :

a) 2001:0001:0002:014e:f140:0102:8012:00ae

b) fc01:1::1

c) 2a01:cb1c:91c:b500:2870:35c8:8a02:e1f3

d) fe80::4def:1d35:c772:282d

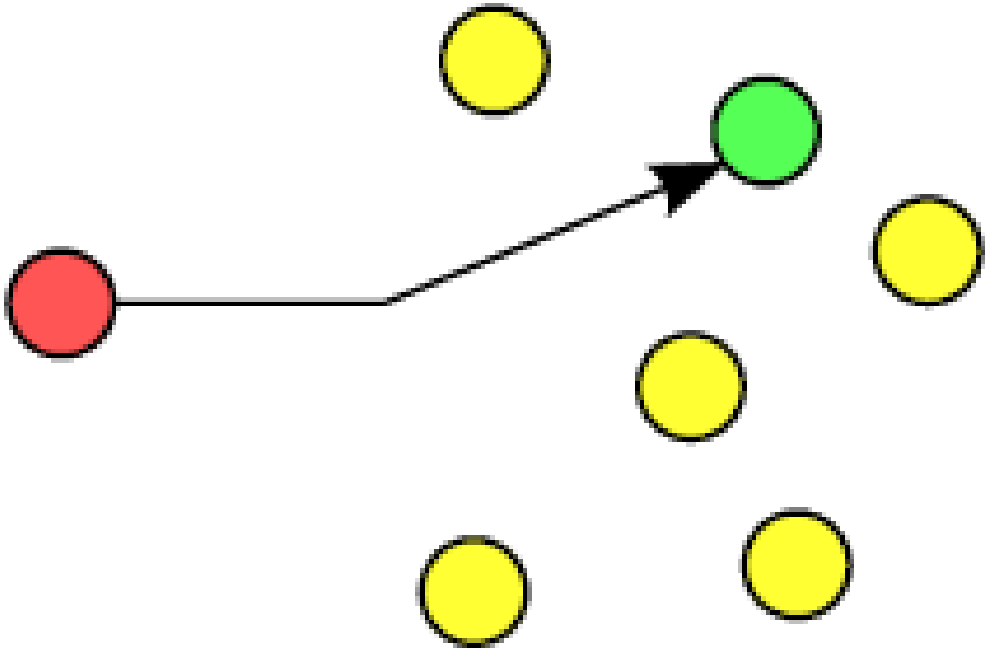
e) ff02::1

f) ::1

g) ff02::2

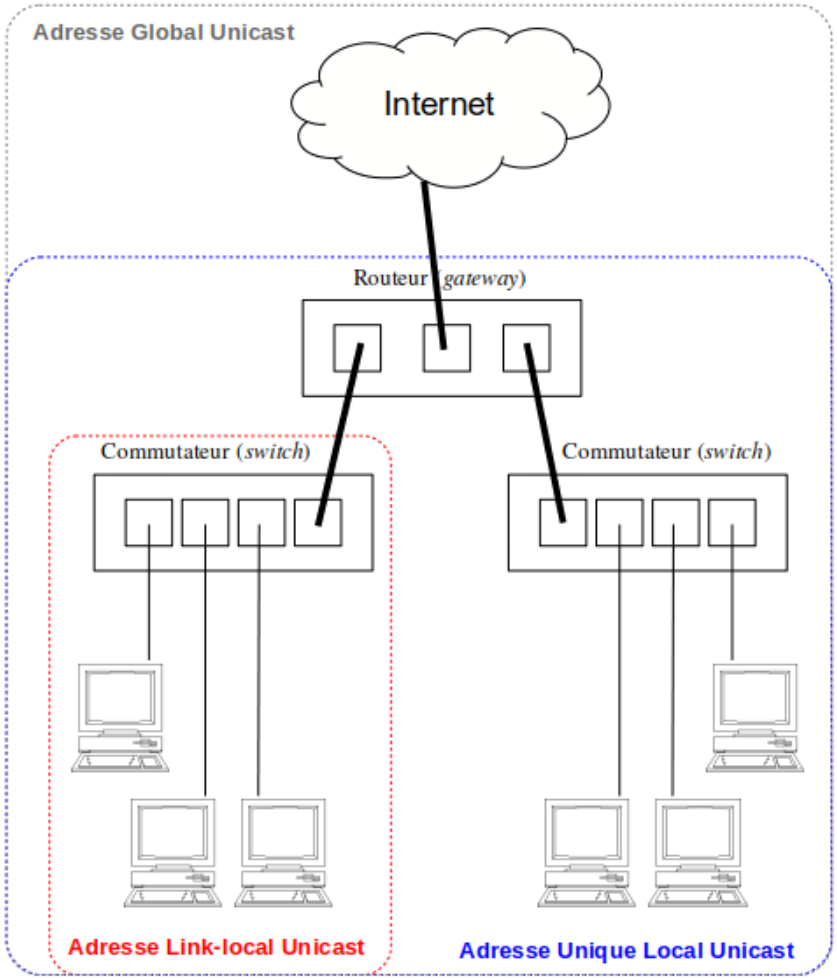
Adresse *unicast*

Il s'agit du même type d'adresse (RFC 4291, section 2.5) qu'en IPv4. C'est donc le type d'adresse le plus classique, composé d'un préfixe réseau à longueur variable suivi d'un identifiant d'interface.
C'est une adresse utilisable comme adresse source ou comme destination.



Type d'adresses *unicast* I

En général, un « nœud » a toujours une adresse *link-local*. Il peut avoir une adresse *unique local*, et une ou plusieurs adresses globales.



Type d'adresses *unicast* II

On distingue trois types d'adresses *unicast* :

- **Global Unicast** : adresse globale. Il s'agit des adresses qui sont uniques dans le monde, et qui sont par conséquent routables sur Internet. Elles se composent d'un préfixe de routage global (/48), suivi du préfixe de sous-réseau (/16) et de l'identifiant d'interface (/64).
- **Link-local Unicast** : adresses de lien local, non-routables en local comme sur Internet. Elles utilisent toutes le préfixe `fe80::/10`. Elles sont systématiquement générées lors de l'utilisation de l'autoconfiguration sans état (*stateless*) et utilisées pour la configuration automatique d'adresse, la découverte de voisin, ou en l'absence d'un routeur. Une adresse *link-local* est utilisée principalement au démarrage et lorsque la machine n'a pas d'autres adresses.

Type d'adresses *unicast* III

- **Unique Local Unicast** : adresses de lien local, non-routables sur Internet. C'est la catégorie qui se rapproche le plus des adresses privées IPv4 (RFC 1918). Elles utilisent toutes le préfixe `fc00::/7`, mais avec le huitième bit en partant de la gauche positionné à 1 si le préfixe est défini localement. Actuellement, elles sont reconnaissables par leur premier bloc qui commence systématiquement par `fd` : `fd00::/8`.

Structure de l'adresse *unicast*

Structure des adresses unicast globales

champ	*préfixe*	*sous-réseau*	*interface*
bits	48	16	64

Structure des adresses link-local

champ	*préfixe*	*zéro*	*interface*
bits	10	54	64

1111111010

Structure des adresses locale unique

champ	*préfixe*	*L*	*ID globale*	*Subnet*	*Interface*
bits	7	1	40	16	64

1111110

Allocation des adresses globales

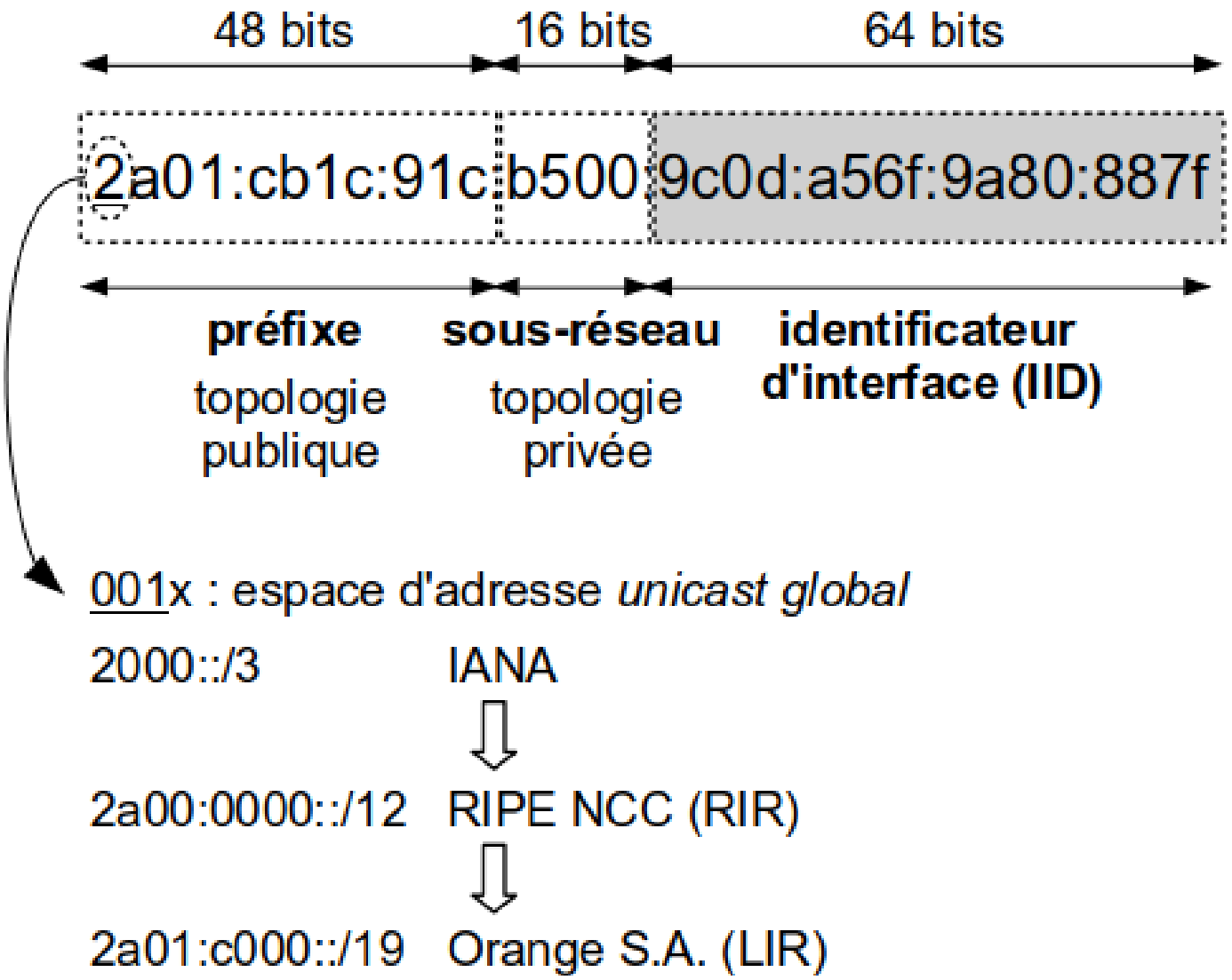
- L'IANA alloue des blocs de taille /23 à /12 dans l'espace *unicast* global (`2xxx::/3`) aux cinq RIR.
  `http://www.iana.org/assignments/ipv6-unicast-address-assignments`
- Les RIR les allouent aux LIR sous forme de blocs jusqu'en /32.
- Le LIR peut à son tour assigner 65536 blocs /48 à ses clients, qui disposent alors chacun de 65536 réseaux /64.

Structure des préfixes distribués

IANA	*RIR*	*LIR*	*Client*	*Sous-réseau*	*Interface*
3	20	9	16	16	64

Remarque : Vu la disponibilité des adresses, l'utilisation du NAT ne sera plus nécessaire.

Exemple d'adresse globale



Durée de vie

- Les adresses IPv6 associées à une interface ont une durée de vie déterminée.
- La durée de vie est en général infinie, mais on peut configurer une durée de vie préférée et une durée de vie de validité.
- Ces durées de vie sont configurées dans les routeurs qui fournissent les préfixes pour la configuration automatique.
- Quand la durée d'utilisation d'une adresse dépasse la durée préférée, elle n'est plus utilisée pour les nouvelles connexions. Elle va progressivement passée par différentes phases : préférée, dépréciée, invalide. Quand sa période de validité est atteinte, elle est supprimée de la configuration de l'interface.

Adresse de boucle locale (*loopback*)

L'**adresse de boucle locale** (*loopback*) est notée ::1.

```
$ cat /etc/hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
```

L'adresse :: correspond logiquement à l'adresse IPv4 `0.0.0.0` et ne sera donc utilisée que pour définir les passerelles par défaut, ou comme adresse source des paquets de découverte de son IP.

Portée de l'adresse IPv6

La portée d'une adresse IPv6 consiste en son domaine de validité et d'unicité.

Pour les adresses *unicast* :

- l'adresse *loopback* ::1/128 a une validité limitée à l'hôte
- les adresses locales de lien, uniques sur un lien donné
- les autres adresses, y compris les adresses locales uniques, ont une portée globale (donc elles sont uniques dans le monde)
- Les adresses *anycast*, dont la portée est identique aux adresses *unicast*

Assignation des adresses d'interface

La taille du sous-réseau étant fixée à 64 bits, les hôtes disposent des 64 bits restants pour la numérotation à l'intérieur du sous-réseau.

- Configuration manuelle : on fixe l'adresse
- Configuration automatique : autoconfiguration sans état **SAA** (*Stateless Address Autoconfiguration*) ou via **DHCPv6**.

Il existe au moins une adresse locale de lien (`fe80::/64`) pour chaque interface IPv6.

Configuration automatique

- Sans état (*Stateless Address Autoconfiguration*) :
  - autoconfiguration avec tirage pseudo aléatoire, l'adresse change dans le temps (RFC 4941),
  - autoconfiguration basée sur une clé secrète et sur le préfixe réseau, ne dévoile pas l'adresse MAC et est stable pour chaque préfixe réseau, c'est l'usage recommandé pour une adresse fixe (RFC 8064, RFC 7217),
  - autoconfiguration basée sur l'adresse MAC (EUI-64), adresse stable mais machine facilement identifiable, usage déconseillé par l'IETF depuis 2017 (RFC 8064, RFC 4862),
- Avec état (*Stateful*) :
  - attribution par un serveur DHCPv6 (RFC 3315).

Adresse MAC (EUI-48 et EUI-64) I

Une adresse MAC (*Media Access Control*) ou adresse physique est un identifiant physique stocké dans une interface réseau.

- Une adresse **EUI-48** (*Extended Unique Identifier*) est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret. Ces 48 bits sont répartis de la façon suivante :
  - 1 bit I/G : 0 indique que l'adresse est individuelle (*unicast*) ou 1 pour une adresse de groupe (*multicast* ou *broadcast*) ;
  - 1 bit U/L : 0 indique que l'adresse est universelle (conforme au format de l'IEEE) ou 1 pour une adresse administrée localement ;
  - 22 bits réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur ;
  - 24 bits : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur).

Adresse MAC (EUI-48 et EUI-64) II

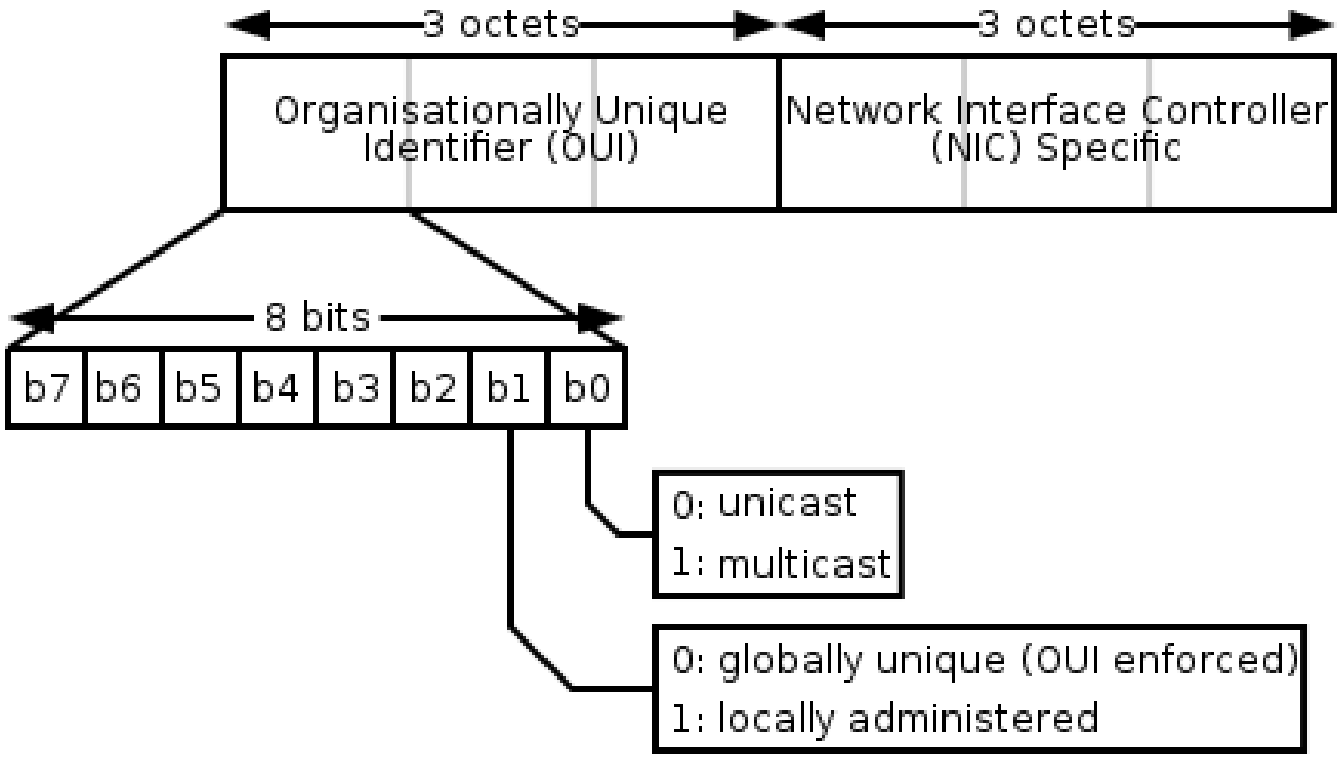


FIGURE – Structure d'une adresse MAC 48 bits

Adresse MAC (EUI-48 et EUI-64) III

- L'adresse **EUI-64** est similaire à celle de EUI-48. Les adresses EUI-64 sont utilisées notamment par IPv6, ZigBee, LoRaWAN, ... Dans le cas d'IPv6, l'adresse EUI-64 est construite à partir de l'adresse EUI-48 en insérant FFFE dans les octets 4 et 5. L'adresse IPv6 utilise un format modifié dans lequel le bit U/L est inversé (*globally unique* : 0 $\rightarrow$ 1) [RFC 2464].

Quelques adresses particulières :

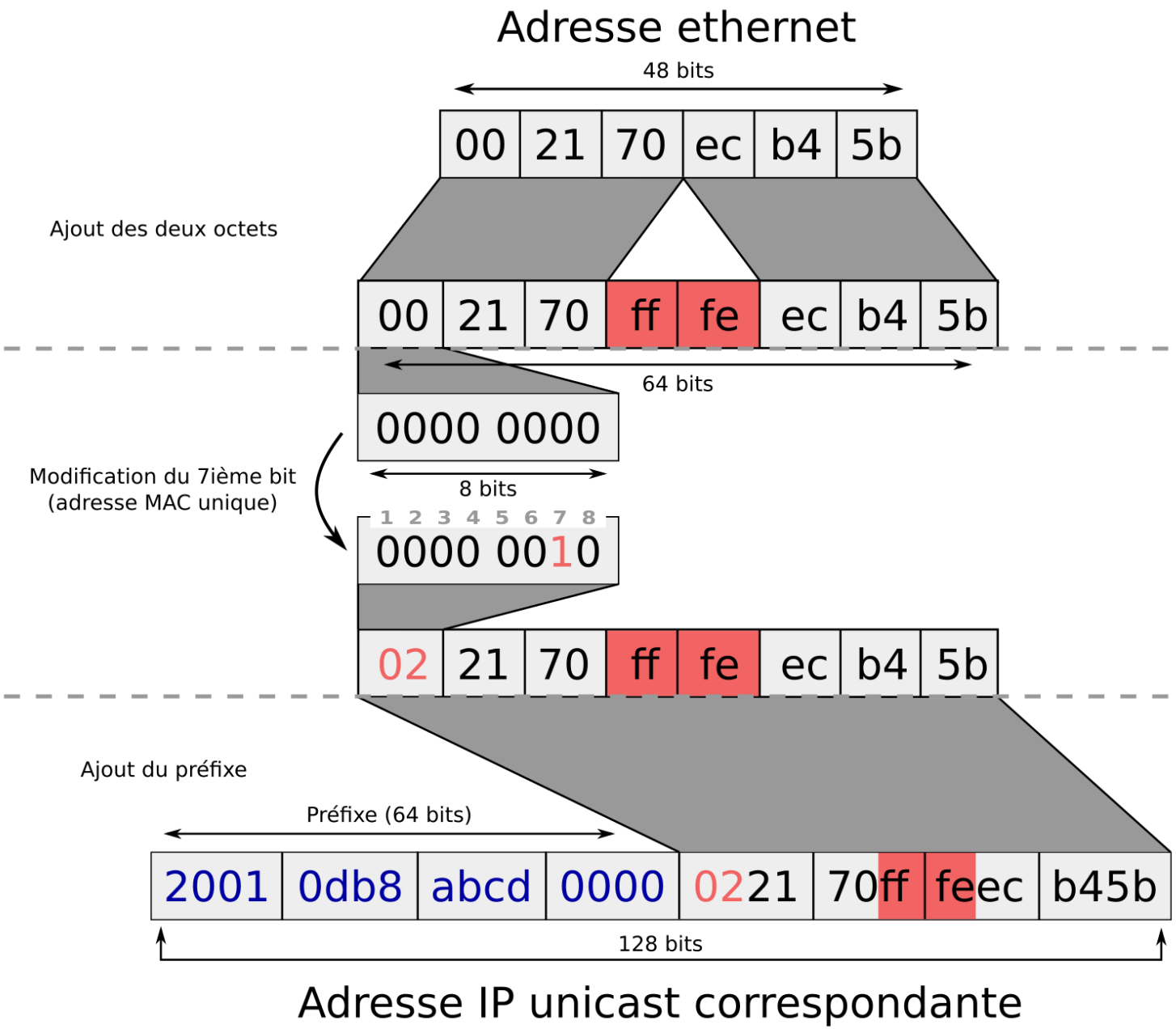
- `FF:FF:FF:FF:FF:FF` : Adresse *broadcast*
- 33:33:`xx:xx:xx:xx` : Adresses *multicast* IPv6
- 01:00:5E:`xx:xx:xx` : Adresses *multicast* IPv4

Autoconfiguration basée sur l'adresse MAC I

La construction automatique de l'adresse IP basée sur l'adresse MAC suit le principe suivant :

- Ajouter les octets `fffe` au milieu de l'adresse MAC de l'interface.
- Positionner le septième bit (U/L) de l'adresse MAC modifiée en partant de la gauche à 1 si l'adresse est unique (ce qui est le cas pour toutes les adresses MAC par défaut) sinon 0.
- Récupération du préfixe si c'est une adresse globale, sinon **utilisation du préfixe d'adresse de lien** local.
- Concaténation du préfixe avec l'adresse MAC ainsi modifiée.

Autoconfiguration basée sur l'adresse MAC II



Excercice n°3 I

I. En fonction de la longueur du préfixe, déterminer l'identifiant de réseau pour les adresses suivantes :

a) 2001:0660:2402:1001:208:2ff:fedc:6133/48

b) 2a01:cb1c:91c:b500:2870:35c8:8a02:e1f3/56

c) 2001:0660:f402:1000:208:2ff:fedc:9033/64

II. Déterminer l'identifiant d'interface pour les adresses suivantes :

a) 2001:0660:2402:1001:208:2ff:fedc:6133/48

b) 2a01:cb1c:91c:b500:2870:35c8:8a02:e1f3/56

c) 2001:0660:f402:1000:208:2ff:fedc:9033/64

Excercice n°3 II

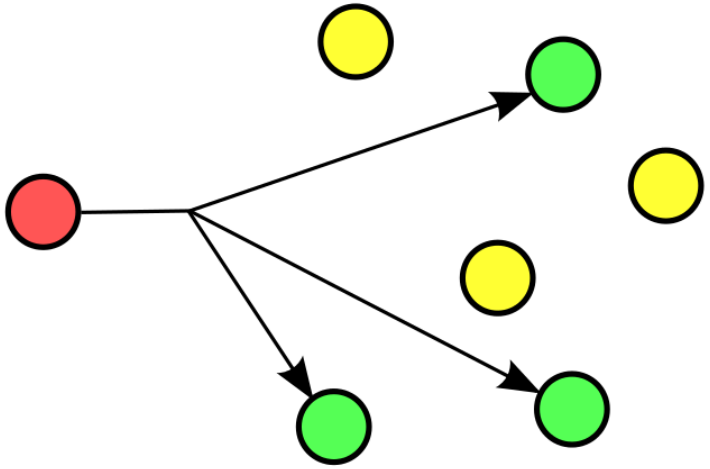
III. Sachant que la longueur du préfixe attribué par le FAI Orange est de /56, combien de sous-réseaux pourra-t-on créer ?

IV. À partir l'adresse IPV6 `2a01:cb1c:91c:b500::/56` fournie par le FAI Orange, proposer une adressage manuel du réseau ci-dessous (on ne tiendra pas compte de l'accès Internet) :

V. Pour le réseau ci-dessus, donner les tables de routage des différents postes (seuls `pc1` et `pc2` possèdent des routes par défaut).

Adresse *multicast* I

Ce type d'adresse (RFC 4291, section 2.7) correspond précisément à celle utilisée en IPv4. Il s'agit d'adresses virtuelles qui distribuent des paquets à tous les membres inscrits dans un groupe. C'est une adresse utilisable comme adresse destination.



Adresse *multicast* II

Rappel : Le *broadcast* a été supprimé, au profit de l'utilisation massive du *multicast*.

Elles utilisent toutes le préfixe `ff00::/8`. Elles sont donc reconnaissables par leur premier bloc qui commence systématiquement par `ff`.

Les adresses multicast ont le format suivant :

Format d'une adresse multicast

champ	*préfixe*	*drap.*	*scope*	*groupe*
bits	8	4	4	112

11111111

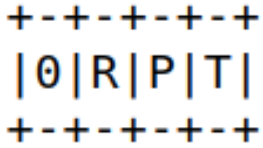
Trois des quatre bits du champ **drapeau** (*flags* ORPT) sont définis par la RFC 4291. Le bit le plus significatif est réservé à un usage ultérieur. Les quatre bits de **portée** (*scope*) indiquent le domaine de validité de l'adresse.

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

Drapeaux (*flags*) de l'adresse *multicast*

Pour les adresses *multicast* `ff00::/8`

Les 4 bits les plus significatifs du 2e octet (`ffx0::`) sont :



- T = 0 : une adresse multicast permanente « bien connu »("well-known"), assignée par l'IANA
- T = 1 : une adresse multicast temporaire (transitoire ou dynamique)
- P = 0 : adresse multicast qui n'est pas assignée en fonction d'un préfixe réseau
- P = 1 : adresse multicast qui est attribuée en fonction du préfixe du réseau. Si P = 1, T DOIT être mis à 1.
- R : voir la RFC 3956
- 0 : le bit de poids fort est réservé et doit être initialisé à 0.

Portée (*scope*) de l'adresse *multicast*

Pour les adresses *multicast* `ff00::/8`

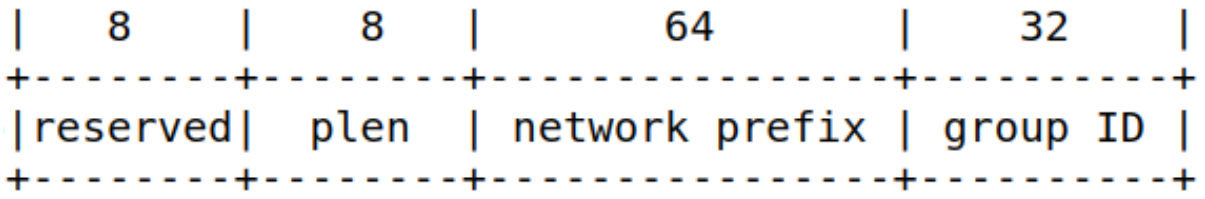
Les 4 bits les moins significatifs du 2e octet (`ff0x::`) identifient la portée de l'adresse :

- x=1 : l'adresse *multicast* est locale à l'hôte,
- x=2 : l'adresse est locale au lien,
- x=5 : l'adresse est locale au site,
- x=8 : l'adresse est locale à l'organisation,
- x=e : l'adresse est globale.

Groupe de *multicast*

Pour les adresses *multicast* `ff00::/8`

Le champ groupe (112 bits) identifie le groupe de *multicast* (permanent ou transitoire) dans la portée donnée.



Des définitions supplémentaires de la structure de ce champ sont fournies dans la RFC 3306.

- *reserved* : doit être fixé à 0x00.
- *plen* : le nombre réel de bits dans le champ de préfixe de réseau qui identifient le sous-réseau lorsque P = 1.
- *network prefix* (64 bits) : identifie le réseau de la portée du *multicast*.
- *group ID* (32 bits) : le groupe de diffusion (généralement une transcription d'une adresse IPv4 *multicast*)

Adresses *multicast* prédéfinies

Un certain nombre d'adresses *multicast* sont normalisées par l'IETF (drapeau T positionné à 0), et sont documentées dans la RFC 2461.

Nom	Adresse	Équivalent IPv4	Fonction
all-nodes	`ff02::1`	`224.0.0.1`	Tous les noeuds et routeurs du lien local (utilisée par exemple pour les interfaces qui n'ont pas encore d'adresse mais qui veulent recevoir une réponse)
all-routers	`ff02::2`	`224.0.0.2`	Tous les routeurs du lien local (utilisée par exemple pour solliciter une annonce de préfixe sur le réseau)

```
$ cat /etc/hosts
...
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Le *multicast* qui se rapproche le plus du *broadcast* traditionnel correspond au groupe *all-nodes* et censé correspondre à tous les noeuds (mais dont l'inscription est à la discrétion de la machine).

Adresses *multicast* connues

Well-known IPv6 multicast addresses

Address	Description
ff02::1	All nodes on the local network segment
ff02::2	All routers on the local network segment
ff02::5	OSPFv3 All SPF routers
ff02::6	OSPFv3 All DR routers
ff02::8	IS-IS for IPv6 routers
ff02::9	RIP routers
ff02::a	EIGRP routers
ff02::d	PIM routers
ff02::16	MLDv2 reports (defined in RFC 3810)
ff02::1:2	All DHCP servers and relay agents on the local network segment (defined in RFC 3315)
ff02::1:3	All LLMNR hosts on the local network segment (defined in RFC 4795)
ff05::1:3	All DHCP servers on the local network site (defined in RFC 3315)
ff0x::c	Simple Service Discovery Protocol
ff0x::fb	Multicast DNS
ff0x::101	Network Time Protocol
ff0x::108	Network Information Service
ff0x::114	Used for experiments

Adresse *multicast* sollicité

- Le protocole ND (*Neighbor Discovery Protocol*) associe les adresses IPv6 à des adresses MAC sur un segment, comme ARP pour IPv4.
- Il utilisera l'adresse *multicast* `ff02::1:ff00:0/104` pour découvrir l'adresse MAC d'un hôte dont l'adresse IPv6 est connue (*solicited node*). En utilisant l'adresse *multicast* sollicité, il sera possible de joindre le destinataire.
- La construction d'une adresse IPv6 *multicast* sollicité concatène le préfixe `ff02::1:ff00:0/104` avec les trois derniers octets (24 derniers bits) de l'adresse IPv6.

Adresse Ethernet *multicast*

L'adresse ethernet (MAC) d'une trame à destination d'un groupe multicast est dérivée de l'adresse IP du groupe (RFC 5342 et 2464) :

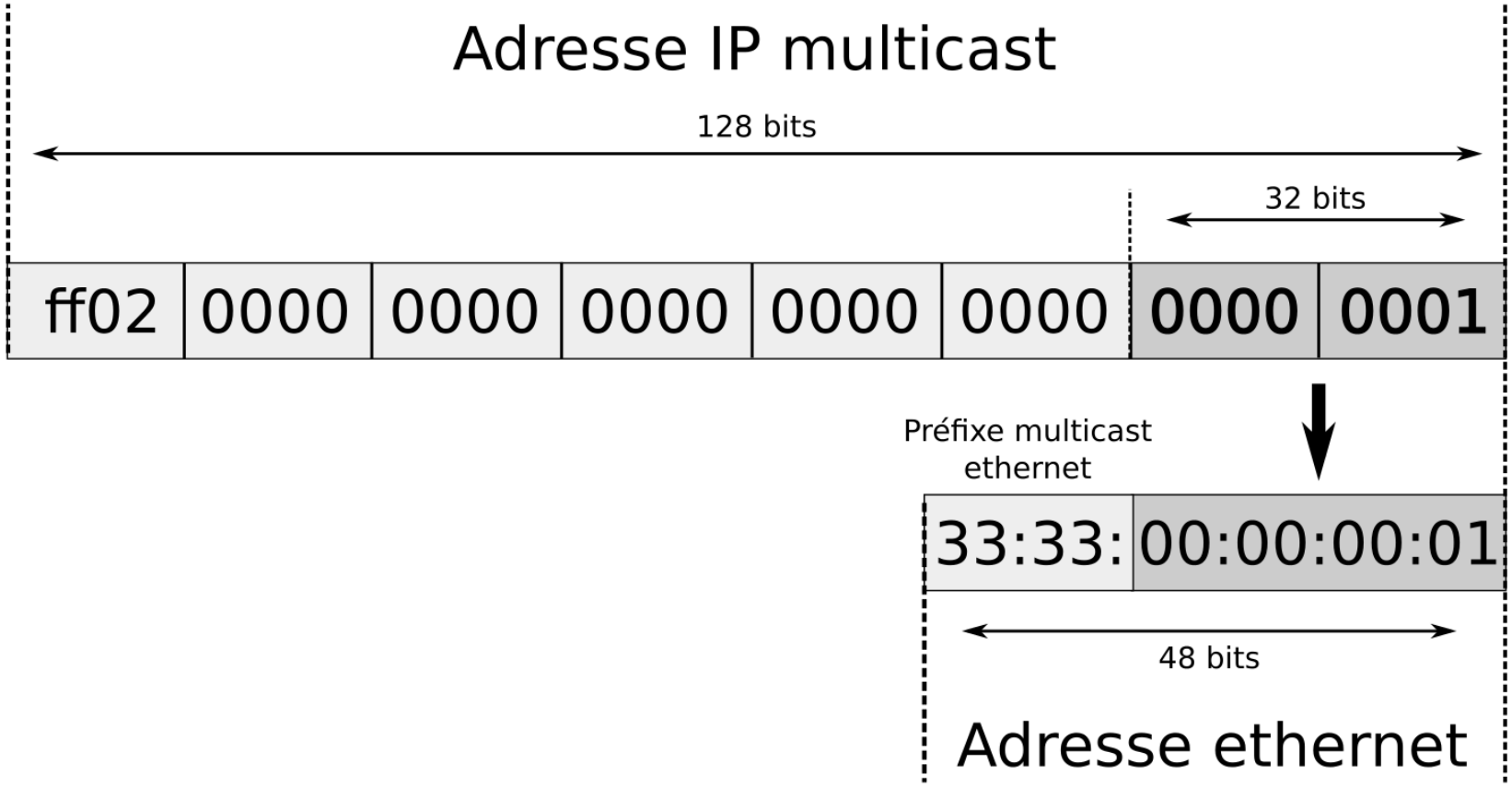


FIGURE – Conversion d'une adresse IP *multicast* en adresse ethernet *multicast* (adresse *all-nodes*)

Excercice n°4

Soit l'adresse multicast IPv6 suivante : `ff1e::e100:0025`

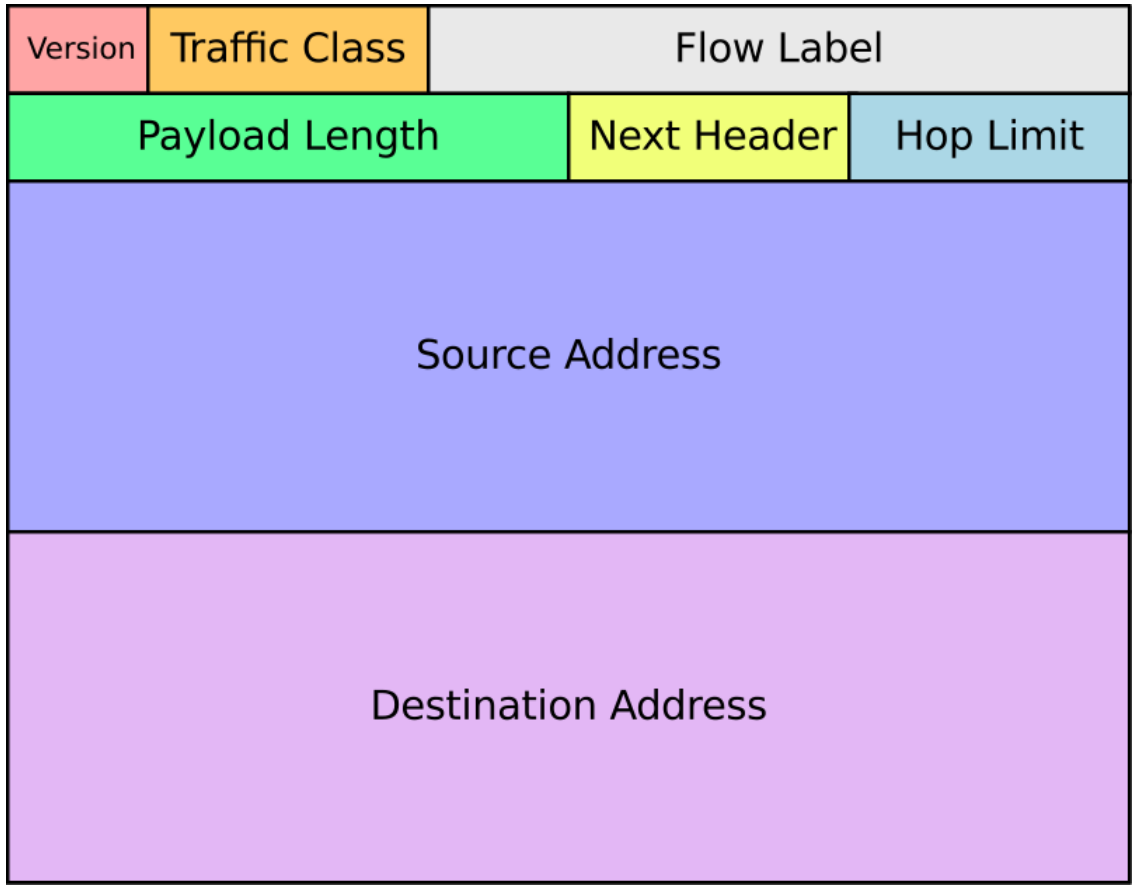
I. Décoder et compléter le tableau ci-dessous :

Unicast	Multicast	Permanente	Temporaire	Portée limitée	Portée globale

II. Le champ *group ID* de l'adresse IPv6 est en fait une adresse IPv4. Exprimer cette adresse en notation décimale pointée.

IPv6

IPv6 (Internet Protocol version 6) est un protocole réseau sans connexion (RFC 2460 et 8200).
L'en-tête du paquet IPv6 est de **taille fixe à 40 octets** (20 octets en IPv4), des options pouvant la porter jusqu'à 60 octets.



Signification des champs IPv6

La signification des champs est la suivante :

- *Version* (4 bits) : fixé à la valeur du numéro de protocole internet, 6
- *Traffic Class* (8 bits) : utilisé dans la qualité de service.
- *Flow Label* (20 bits) : permet le marquage d'un flux pour un traitement différencié dans le réseau.
- *Payload length* (16 bits) : taille de la charge utile en octets.
- *Next Header* (8 bits) : identifie le type de header qui suit immédiatement selon la même convention qu'IPv4.
- *Hop Limit* (8 bits) : décrémenté de 1 par chaque routeur, le paquet est détruit si ce champ atteint 0 en transit.
- *Source Address* (128 bits) : adresse source
- *Destination Address* (128 bits) : adresse destination.

Champ *Next Header*

Le champ *Next Header* identifie le prochain en-tête. Il peut s'agir :

- d'un protocole (ICMP, UDP, TCP, etc.)
- ou d'une extension. Les extensions contiennent aussi ce champ pour permettre un chaînage.

Valeur	Extension
0	proche en proche
43	routage
44	fragmentation
50	confidentialité
51	authentification
59	fin des en têtes
60	destination
135	mobilité IPv6

Valeur	Protocole
6	TCP
17	UDP
41	IPv6
58	ICMPv6

Capture d'un paquet IPv6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	2001:db8:46::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:46::1 from 0e:ab:f8:0c:10:4b
2	0.004	2001:db8:46::1	2001:db8:46::2	ICMPv6	86	Neighbor Advertisement 2001:db8:46::1 (sol, ovr) is at 6e:5f:98:37:0c:07
3	0.004	2001:db8:46::2	2001:db8:46::1	ICMPv6	118	Echo (ping) request id=0xe401, seq=1
4	0.004	2001:db8:46::1	2001:db8:46::2	ICMPv6	118	Echo (ping) reply id=0xe401, seq=1
5	4.999	fe80::6c5f:98ff:fe37:c07	2001:db8:46::2	ICMPv6	86	Neighbor Solicitation for 2001:db8:46::2 from 6e:5f:98:37:0c:07
6	4.999	2001:db8:46::2	fe80::6c5f:98ff:fe37:c07	ICMPv6	78	Neighbor Advertisement 2001:db8:46::2 (sol)
7	9.995	fe80::cab:f8ff:fe0c:104b	fe80::6c5f:98ff:fe37:c07	ICMPv6	86	Neighbor Solicitation for fe80::6c5f:98ff:fe37:c07 from 0e:ab:f8:0c:10:4b
8	9.995	fe80::6c5f:98ff:fe37:c07	fe80::cab:f8ff:fe0c:104b	ICMPv6	78	Neighbor Advertisement fe80::6c5f:98ff:fe37:c07 (sol)
9	14.990	fe80::6c5f:98ff:fe37:c07	fe80::cab:f8ff:fe0c:104b	ICMPv6	86	Neighbor Solicitation for fe80::cab:f8ff:fe0c:104b from 6e:5f:98:37:0c:07
10	14.990	fe80::cab:f8ff:fe0c:104b	fe80::6c5f:98ff:fe37:c07	ICMPv6	78	Neighbor Advertisement fe80::cab:f8ff:fe0c:104b (sol)

```
▸ Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
▾ Ethernet II, Src: 0e:ab:f8:0c:10:4b (0e:ab:f8:0c:10:4b), Dst: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07)
  ▸ Destination: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07)
  ▸ Source: 0e:ab:f8:0c:10:4b (0e:ab:f8:0c:10:4b)
    Type: IPv6 (0x86dd)
▾ Internet Protocol Version 6, Src: 2001:db8:46::2 (2001:db8:46::2), Dst: 2001:db8:46::1 (2001:db8:46::1)
  ▸ 0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 64
    Next header: ICMPv6 (0x3a)
    Hop limit: 64
    Source: 2001:db8:46::2 (2001:db8:46::2)
    Destination: 2001:db8:46::1 (2001:db8:46::1)
▾ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x208b [correct]
    Identifier: 0xe401
    Sequence: 1
    [Response In: 4]
  ▸ Data (56 bytes)
```

```
0000  6e 5f 98 37 0c 07 0e ab  f8 0c 10 4b 86 dd 60 00   n_.7.... ...K..`.
0010  00 00 00 40 3a 40 20 01  0d b8 00 46 00 00 00 00   ...@:@ . ...F....
0020  00 00 00 00 00 02 20 01  0d b8 00 46 00 00 00 00   ...... . ...F....
0030  00 00 00 00 00 01 80 00  20 8b e4 01 00 01 f3 42   ........  ......B
0040  d6 4e 5e 61 0c 00 08 09  0a 0b 0c 0d 0e 0f 10 11   .N^a.... ........
0050  12 13 14 15 16 17 18 19  1a 1b 1c 1d 1e 1f 20 21   ........ ...... !
0060  22 23 24 25 26 27 28 29  2a 2b 2c 2d 2e 2f 30 31   "#$%&'() *+,-./01
0070  32 33 34 35 36 37                                 234567
```

FIGURE – Capture d'un `ping6` (*echo request*)

Analyse de la capture du paquet IPv6

- Le champ `Type` de la trame Ethernet_II indique par un code (`0x86dd`) le protocole de couche supérieure ici **IPv6**.
- Le champ `Version` indique la version du protocole IP ici `6`.
- Le champ `Next header` indique par un code (`0x3a` donc 58) le protocole de couche supérieure ici **ICMPv6**.
  Vérification : `cat /etc/protocols | grep ICMP`
- Le champ `Payload length` indique la longueur en octets du champ *data* du paquets IPv6 ici `0x0040` soit **64 octets**.
- Le champ *data* contient ici un message ICMPv6 : une demande d'écho (type = 128)

Excercice n°5

Soit la capture ci-dessous réalisée avec *Wireshark* :

```
0000 2c 39 96 21 d3 62 2c fd a1 bb bc 0f 86 dd 60 0f
0010 95 a2 00 14 06 40 2a 01 cb 1c 09 1c b5 00 31 a6
0020 57 01 5a e2 3a e7 26 03 10 26 01 00 00 15 00 00
0030 00 00 00 00 00 02 99 64 03 e1 4d 5b 87 f5 b4 43
0040 a6 57 50 10 01 52 d8 65 00 00
```

I. Identifier les adresses MAC Destination et Source.

II. Identifier le type de paquet transporté.

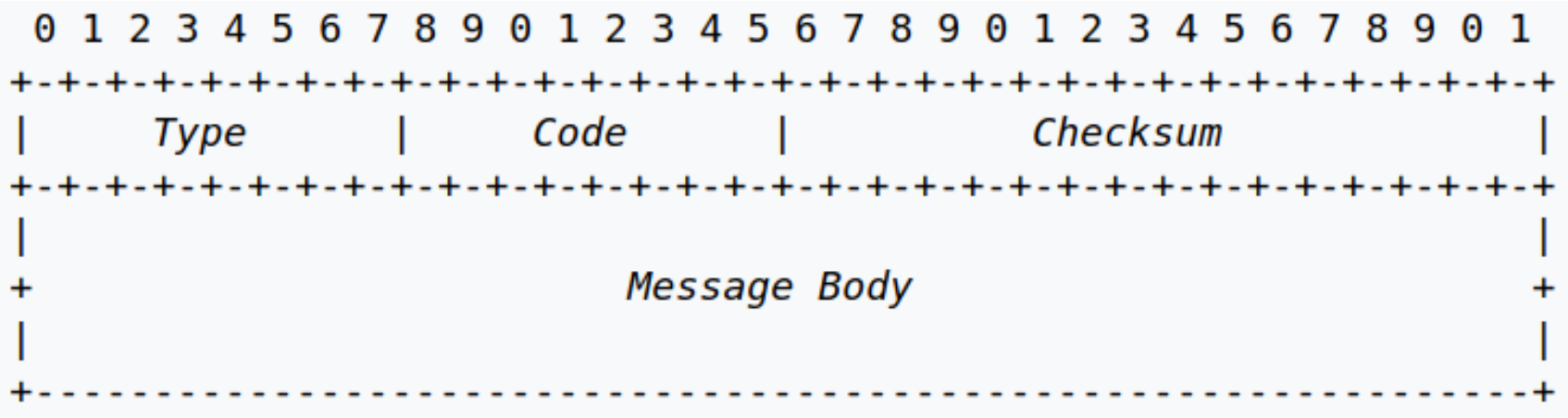
III. Identifier les valeurs de champs *Payload length* et *Next Header*. Préciser leur signification.

IV. Identifier les adresses IP Source et Destination. Quelles sont leur type ?

ICMPv6 (*Internet Control Message Protocol*)

- ICMPv6 fait partie de l'architecture IPv6. Le protocole a été redéfini par la RFC 4443.
- ICMPv6 regroupe maintenant des fonctionnalités de différents protocoles (ICMPv4, IGMP (*Internet Group Membership Protocol*), et ARP (*Address Resolution Protocol*))
- Il a été simplifié en supprimant des types de messages qui ne sont plus utilisés.
- Il intègre des nouveaux types de messages pour des nouvelles fonctionnalités (découverte des routeurs et des préfixes routés, le MTU, de détecter les adresses dupliquées, les hôtes devenus inaccessibles et l'autoconfiguration des adresses).
- Les messages ICMP sont transportés à l'intérieur de paquets IPv6 : un message ICMP est identifié par sa valeur 58 (0x3A) positionnée dans le champ *Next Header* de l'en-tête IPv6.

Message ICMPv6



- *Type* : nature du paquet ICMPv6
  - $\leq 127 \rightarrow$ message d'erreur
  - $> 127 \rightarrow$ message d'information
- *Code* : cause du message ICMPv6 (dépend du *Type*)
- *Checksum* : somme de contrôle (pour détecter des erreurs dans le message ICMP à l'intérieur du message IPv6)

Types de message ICMPv6

Type	Signification	
1	*Destination Unreachable*	**Messages d'erreur**
2	*Packet Too Big*	
3	*Time Exceeded*	
4	*Parameter Problem*	
128	*Echo Request*	**Messages informatifs** Diagnostic (ping)
129	*Echo Reply*	
130	*Group Membership Query*	Gestion des groupes multicast
131	*Group Membership Report*	
132	*Group Membership Reduction*	
133	*Router Solicitation*	Découverte des voisins (*Neighbor Discovery*)
134	*Router Advertisement*	
135	*Neighbor Solicitation*	
136	*Neighbor Advertisement*	
137	*Redirect*	

Etc ...

http://www.iana.org/assignments/icmpv6-parameters

Nouveaux protocoles

- Protocole ND (*Neighbor Discovery Protocol*) [RFC 2461] : pour la découverte des voisins, adresses MAC (ARP), des routeurs
- Protocole SAA (*Stateless Address Autoconfiguration Protocol*) [RFC 4862 et 2462] : pour construire une adresse IPv6 simplement
- Protocole pMTU (*Path MTU discovery*) [RFC 1981] : pour déterminer la taille du MTU afin d'éviter la fragmentation des paquets
- Protocole DHCPv6 (*Dynamic Host Configuraton Protocol*) [RFC 1541]

Remarque : Dans la version IPv6, les protocoles ARP et RARP ne sont plus utilisés et sont remplacés par un protocole de découverte des voisins, appelé ND (*Neighbor Discovery*), qui est un sous-ensemble du protocole de contrôle ICMPv6.

Protocole ND (*Neighbor Discovery Protocol*)

- Le protocole ND est un protocole utilisé par IPv6.
- Il définit cinq types de messages ICMPv6 :

Type	Signification
133	*Router Solicitation*
134	*Router Advertisement*
135	*Neighbor Solicitation*
136	*Neighbor Advertisement*
137	*Redirect*

- ND utilise l'adressage *multicast*.

Les fonctionnalités de ND

NDP définit des mécanismes qui permettent les fonctions suivantes :

- *Router Discovery* : détecte les routeurs sur les liens,
- *Prefix Discovery* : découverte des préfixes sur les liens,
- *Parameter Discovery* : découverte de paramètres comme le MTU,
- *Address Autoconfiguration* : assignation automatique d'adresse sans état,
- *Address Resolution* : établissement de la correspondance entre adresse IP et adresse MAC,
- *Next-hop determination* : détermination du routeur pour une destination déterminée,
- *Neighbor Unreachability Detection* : détermine qu'un hôte n'est plus accessible,
- *Duplicate Address Detection* : détermine si un autre hôte utilise la même adresse IP,
- *Redirect* : information qu'un autre routeur sur le lien fournit un meilleur *next hop*.

Auto-configuration sans état (*stateless*)

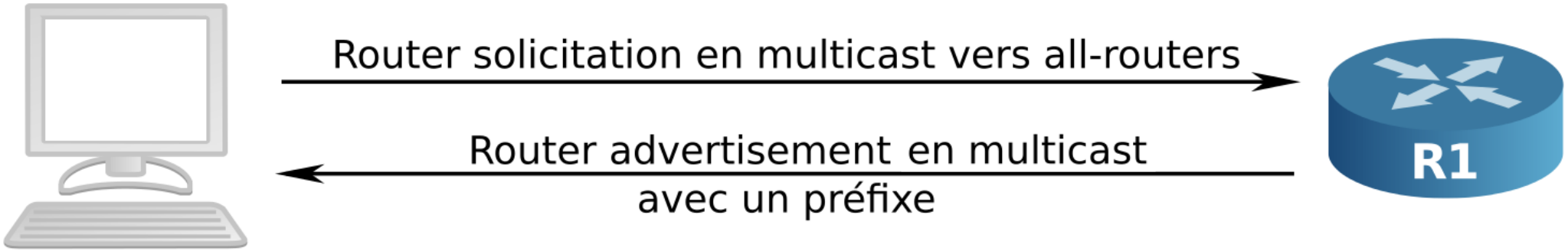
Le protocole SAA (*Stateless Address Autoconfiguration Protocol*) ou SLAAC (*StateLess Address AutoConfiguration*) [RFC 4862 et 2462] permet de construire une adresse IPv6 simplement.

- Avec une auto-configuration sans état, seul le préfixe réseau est donné en recevant des messages RA (*Router Advertisement*). La machine peut les solliciter en envoyant des messages RS (*Router Solicitation*).
- Ensuite, l'équipement aura la charge de générer le suffixe de l'adresse. La machine concatène le préfixe reçu à un identificateur d'interface pour obtenir une adresse IPv6. L'identificateur d'interface (RFC 4291) est fabriqué :
  - par tirage pseudo aléatoire, usage par défaut maintenant (RFC 4941),
  - en se basant sur une clé secrète, usage recommandé pour une adresse fixe (RFC 8064, RFC 7217),
  - en se basant sur l'adresse MAC (EUI-64), déconseillé depuis 2017 (RFC 8064, RFC 4862)

Remarque : la procédure DAD (*Duplicate Address Detection*) permet de s'assurer que l'adresse obtenue est bien unique en envoyant un NS (*Neighbor Solicitation*) [RFC 4861].

Exemple : *Prefix Discovery*

- La machine (`fe80::5074:4cff:fe66:b3d5`) envoie un message *Router Solicitation* vers l'adresse multicast `ff02::2` (=> *ip6-allrouters*) donc à destination de tous les routeurs du lien local.
- R1 (`fe80::3047:cbff:fe52:16e2`) envoie un message *Router Advertisement* vers une adresse multicast (`ff02::1` => *ip6-allnodes*) à destination de tous les noeuds du lien local.



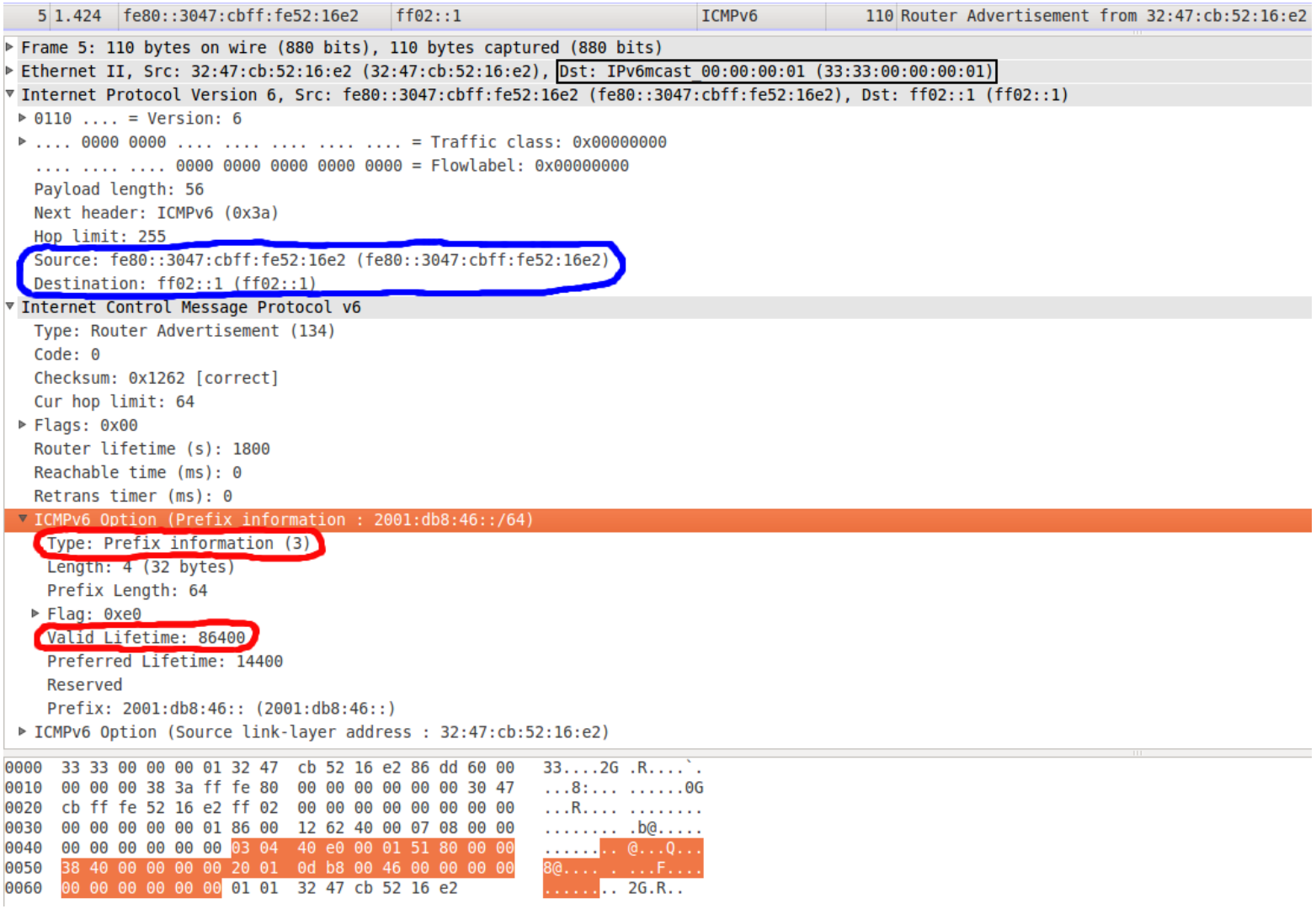
Capture d'un message *Router Solicitation*

```
   4 1.422  fe80::5074:4cff:fe66:b3d5   ff02::2                  ICMPv6      70 Router Solicitation from 52:74:4c:66:b3:d5
▸ Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▸ Ethernet II, Src: 52:74:4c:66:b3:d5 (52:74:4c:66:b3:d5), Dst: IPv6mcast_00:00:00:02 (33:33:00:00:00:02)
▾ Internet Protocol Version 6, Src: fe80::5074:4cff:fe66:b3d5 (fe80::5074:4cff:fe66:b3d5), Dst: ff02::2 (ff02::2)
  ▸ 0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 16
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source: fe80::5074:4cff:fe66:b3d5 (fe80::5074:4cff:fe66:b3d5)
    Destination: ff02::2 (ff02::2)
▾ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0xd9cd [correct]
    Reserved: 00000000
  ▾ ICMPv6 Option (Source link-layer address : 52:74:4c:66:b3:d5)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: 52:74:4c:66:b3:d5 (52:74:4c:66:b3:d5)
```

```
0000  33 33 00 00 00 02 52 74  4c 66 b3 d5 86 dd 60 00   33....Rt Lf....`.
0010  00 00 00 10 3a ff fe 80  00 00 00 00 00 00 50 74   ....:... ......Pt
0020  4c ff fe 66 b3 d5 ff 02  00 00 00 00 00 00 00 00   L..f.... ........
0030  00 00 00 00 00 02 85 00  d9 cd 00 00 00 00 01 01   ........ ........
0040  52 74 4c 66 b3 d5                                 RtLf..
```

Capture d'un message *Router Advertisement*

Le message ICMPv6 envoyé par R1 contient le *Prefix information* (2001:db8:46::/64). Sa durée de vie est de 86400 secondes soit 24 heures.



Exemple : *Address Resolution*

- Le protocole ND permet d'associer les adresses IPv6 à des adresses MAC sur un segment, comme ARP pour IPv4.
- Le message *Neighbor Solicitation* (Type : 135) permet de demander sur le lien local à quelle adresse MAC correspond l'adresse IPv6.
- Le poste qui fait une requête "*neighbor sollicitation*" fournit son adresse MAC pour que la réponse se fasse en *unicast*. La requête utilise un adressage *multicast* :
  - Adresse MAC destination : `33:33:ff:00:00:01` (*multicast*)
  - Adresse IPv6 destination : `ff02::1:ff00:1` (*multicast solicited node*)
- La construction d'une adresse IPv6 *multicast* sollicité concatène le préfixe `ff02::1:ff00:0/104` avec les trois derniers octets (24 derniers bits) de l'adresse IPv6.
- Le poste ayant reconnu une de ses adresses IPv6 (en écoutant sur tous ses groupes *multicast*) répond par un message *Neighbor Advertisement* (Type : 136) et envoie son adresse MAC.

Capture d'un message *Neighbor Solicitation*

Demande en *multicast* sur le lien local à quelle adresse MAC correspond l'adresse IPv6 2001:db8:46::1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:db8:46::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:46::1 from 0e:ab:f8:0c:10:4b
2	0.004018	2001:db8:46::1	2001:db8:46::2	ICMPv6	86	Neighbor Advertisement 2001:db8:46::1 (sol, ovr) is at 6e:5f:98:37:0c:07
3	0.004206	2001:db8:46::2	2001:db8:46::1	ICMPv6	118	Echo (ping) request id=0xe401, seq=1, hop limit=64 (reply in 4)
4	0.004303	2001:db8:46::1	2001:db8:46::2	ICMPv6	118	Echo (ping) reply id=0xe401, seq=1, hop limit=64 (request in 3)

```
▸ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▸ Ethernet II, Src: 0e:ab:f8:0c:10:4b (0e:ab:f8:0c:10:4b), Dst: IPv6mcast_ff:00:00:01 (33:33:ff:00:00:01)
▸ Internet Protocol Version 6, Src: 2001:db8:46::2, Dst: ff02::1:ff00:1
▾ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x069a [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: 2001:db8:46::1
  ▸ ICMPv6 Option (Source link-layer address : 0e:ab:f8:0c:10:4b)
```

```
0000  33 33 ff 00 00 01 0e ab  f8 0c 10 4b 86 dd 60 00   33·····  ···K··`·
0010  00 00 00 20 3a ff 20 01  0d b8 00 46 00 00 00 00   ··· :· ·  ···F····
0020  00 00 00 00 00 02 ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 01 ff 00 00 01 87 00  06 9a 00 00 00 00 20 01   ········ ······ ·
0040  0d b8 00 46 00 00 00 00  00 00 00 00 00 01 01 01   ···F···· ········
0050  0e ab f8 0c 10 4b                                 ·····K
```

Capture d'un message *Neighbor Advertisement*

Réponse en *unicast* contenant l'adresse MAC 6e:5f:98:37:0c:07 correspondant à l'adresse IPv6 2001:db8:46::1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:db8:46::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:46::1 from 0e:ab:f8:0c:10:4b
2	0.004018	2001:db8:46::1	2001:db8:46::2	ICMPv6	86	Neighbor Advertisement 2001:db8:46::1 (sol, ovr) is at 6e:5f:98:37:0c:07
3	0.004206	2001:db8:46::2	2001:db8:46::1	ICMPv6	118	Echo (ping) request id=0xe401, seq=1, hop limit=64 (reply in 4)
4	0.004303	2001:db8:46::1	2001:db8:46::2	ICMPv6	118	Echo (ping) reply id=0xe401, seq=1, hop limit=64 (request in 3)

```
▸ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▸ Ethernet II, Src: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07), Dst: 0e:ab:f8:0c:10:4b (0e:ab:f8:0c:10:4b)
▸ Internet Protocol Version 6, Src: 2001:db8:46::1, Dst: 2001:db8:46::2
▾ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0x7904 [correct]
    [Checksum Status: Good]
  ▸ Flags: 0x60000000, Solicited, Override
    Target Address: 2001:db8:46::1
  ▸ ICMPv6 Option (Target link-layer address : 6e:5f:98:37:0c:07)
```

```
0000  0e ab f8 0c 10 4b 6e 5f  98 37 0c 07 86 dd 60 00   .....Kn_ .7....`.
0010  00 00 00 20 3a ff 20 01  0d b8 00 46 00 00 00 00   ... :. .  ...F....
0020  00 00 00 00 00 01 20 01  0d b8 00 46 00 00 00 00   ...... .  ...F....
0030  00 00 00 00 00 02 88 00  79 04 60 00 00 00 20 01   ........ y.`... .
0040  0d b8 00 46 00 00 00 00  00 00 00 00 00 01 02 01   ...F.... ........
0050  6e 5f 98 37 0c 07                                 n_.7..
```

Protocole pMTU (*Path MTU discovery*)

- pMTU (*Path MTU discovery*) est une technique permettant de déterminer la taille du MTU (*Maximum Transmission Unit*) afin d'éviter la fragmentation des paquets qui affecte la performance des routeurs.
- Il permet la découverte automatique du pMTU pour un chemin donné.
- Il utilise des messages ICMPv6 : "*Packet size Too Large*" (type 2 contenant une nouvelle valeur de MTU)
- Il est défini pour ICMPv6 par la RFC 8201.

Excercice n°6

I. Quelle est la portée de l'adresse IPv6 multicast `ff02::1` ? Donner l'adresse MAC multicast correspondant à cette adresse ?

II. Quelle est la valeur du bit T de l'adresse IPv6 multicast `ff02::2` ? Donner l'adresse MAC multicast correspondant à cette adresse ?

DHCPv6 (*Dynamic Host Configuration Protocol*)

- DHCPv6 est un protocole de configuration dynamique pour IPv6 (RFC 3315).
- Il utilise le port UDP numéro 546 du côté client et le port UDP numéro 547 du côté serveur.
- Principe de base :
  - le client DHCPv6 envoie une sollicitation (*Solicit*) vers l'adresse multicast `[ff02::1:2]:547`
  - le serveur DHCPv6 répond avec une annonce (*Advertise*)
  - le client DHCPv6 répond avec une demande (*Request*) vers l'adresse multicast `[ff02::1:2]:547`
  - le serveur DHCPv6 termine avec une réponse (*Reply*)

Échanges DHCPv6

Le client envoie les messages *Solicit* et *Request* vers l'adresse *multicast* de lien local `ff02::1:2` (*All DHCP Relay Agents and Servers* [RFC8415])

No.	Time	Source	Destination	Protocol	Length	Info
9	184.307849	fe80::6c5f:98ff:fe37:c07	ff02::1:2	DHCPv6	114	Solicit XID: 0x48d49c CID: 0001000116695baa6e5f9837
10	184.324358	fe80::d49e:7aff:fed6:2ec7	ff02::1:ff37:c07	ICMPv6	86	Neighbor Solicitation for fe80::6c5f:98ff:fe37:c07
11	184.324673	fe80::6c5f:98ff:fe37:c07	fe80::d49e:7aff:fed6:2ec7	ICMPv6	86	Neighbor Advertisement fe80::6c5f:98ff:fe37:c07 (so
12	184.324857	fe80::d49e:7aff:fed6:2ec7	fe80::6c5f:98ff:fe37:c07	DHCPv6	199	Advertise XID: 0x48d49c IAA: 2001:db8:46::20 CID: 0
13	185.367200	fe80::6c5f:98ff:fe37:c07	ff02::1:2	DHCPv6	160	Request XID: 0x6feed3 CID: 0001000116695baa6e5f9837
14	185.369244	fe80::d49e:7aff:fed6:2ec7	fe80::6c5f:98ff:fe37:c07	DHCPv6	199	Reply XID: 0x6feed3 IAA: 2001:db8:46::20 CID: 00010

```
▸ Frame 9: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
▸ Ethernet II, Src: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
▸ Internet Protocol Version 6, Src: fe80::6c5f:98ff:fe37:c07, Dst: ff02::1:2
▸ User Datagram Protocol, Src Port: 546, Dst Port: 547
▸ DHCPv6
```

Excercice n°7

Dans la capture précédente des échanges DHCPv6 :

I. Quelle est l'adresse IP du serveur DHCP ? Quel est son type ?

II. Quel est le type de l'adresse `ff02::1:2` ?

III. Justifier l'adresse MAC destination utilisée dans le message *Solicit*.

IV. Quelle est l'adresse IPv6 proposée par le serveur ?

Commandes Linux I

- Visualisation de la configuration des interfaces :

```
$ ifconfig

$ ip -6 addr ls dev lo
$ ip -6 addr ls dev eth0
$ ip -6 addr ls dev enp4s0
$ ip -6 maddress show dev enp4s0
```

Commandes Linux II

- Visualisation des routes :

```
$ route -A inet6
$ route -6
$ route --inet6
$ netstat -6 -rn
$ ip -6 route
```

Commandes Linux III

- Visualisation des voisins :

```
# Comme le cache arp (IPv4)
$ ip -f inet6 neigh
$ ip neigh show

# Tous les noeuds présents sur le lien local
$ ping6 -I enp4s0 ff02::1
$ ping6 ff02::1%enp4s0

# Tous les routeurs présents sur le lien local
$ ping6 -I enp4s0 ff02::2

# Tous les routeurs du site
$ ping6 -I enp4s0 ff05::2
```

Commandes Linux IV

- Format et calcul :

```
$ man ipv6calc

$ ipv6calc --showinfo 2a01:cb1c:91c:b500:9c0d:a56f:9a80:887
    f
$ ipv6calc --showinfo -m -i 2a01:cb1c:91c:b500:9c0d:a56f:9
    a80:887f
$ ipv6calc --showinfo --show_types

$ ipv6calc --addr_to_uncompressed ::1

$ ipv6calc -q --action conv6to4 --in ipv4 192.168.52.12 --
    out ipv6
```

Commandes Linux V

- Tests :

```
# Google ?
$ ping6 2001:4860:4860::8888
$ whois 2001:4860:4860::8888
$ traceroute6 2001:4860:4860::8888
$ tracepath 2001:4860:4860::8888
$ tracepath6 2001:4860:4860::8888

# Mon adresse IPv6 ?
$ wget -q -O - https://ipv4v6.lafibre.info/ip.php
```

Commandes Linux VI

- Affichage des informations et statistiques réseaux :

```
$ netstat -g6n
$ netstat -natup -A inet6
...
```

- Filtrage des paquets :

```
$ sudo ip6tables -L
```

Commandes Linux VII

- Capturer (*sniffer*) des trames :

```
$ sudo tcpdump -i enp4s0 -vv ip6
```

- Configuration :

```
# Ajout d'une adresse IPv6
$ ifconfig eth0 inet6 add 2001:db8:46::1/64

# Ajout d'une route
$ route -A inet6 add 2001:db8:64::/64 gw 2001:db8:46::2 dev
    eth0
$ ip -6 route add 2001:db8:64::/64 via 2001:db8:46::2 dev
   eth0
```

Commandes Windows I

- Configuration :

```
# Ajout d'une adresse IPv6
ipv6 adu ..

# Ajout d'une route
ipv6 rtu ...

# Autre
netsh
> interface ipv6
```

Commandes Windows II

- Visualisation :

```
# Interfaces
ipv6 if

# Routes
ipv6 rt
```

Commandes Windows III

- Tests :

```
# Google ?
ping6 2001:4860:4860::8888

tracert6 2001:4860:4860::8888
```

Références

Les définitions des adresses IP versions 4 et 6, la notion de classe et la notation CIDR sont documentées dans les **RFC (*Request for comments*)** suivants :

1. Communes
   - RFC 997 - Internet numbers, mars 1987
   - RFC 791 - Internet Protocol, septembre 1981 (IP).
   - RFC 1519 - Classless Inter-Domain Routing (CIDR) : an Address Assignment and Aggregation Strategy, septembre 1993
   - RFC 1918 - Address Allocation for Private Internets, février 1996
   - RFC 1531 - Dynamic Host Configuration Protocol, octobre 1993 (DHCP).
2. IPv4
   - RFC 3330 - Special-Use IPv4 Addresses, septembre 2002
   - RFC 903 - A Reverse Address Resolution Protocol, juin 1984 (RARP).
3. IPv6
   - RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, décembre 1998
   - RFC 2373 - IP Version 6 Addressing Architecture, juillet 1998
   - RFC 2893 - Transition Mechanisms for IPv6 Hosts and Routers, août 2000