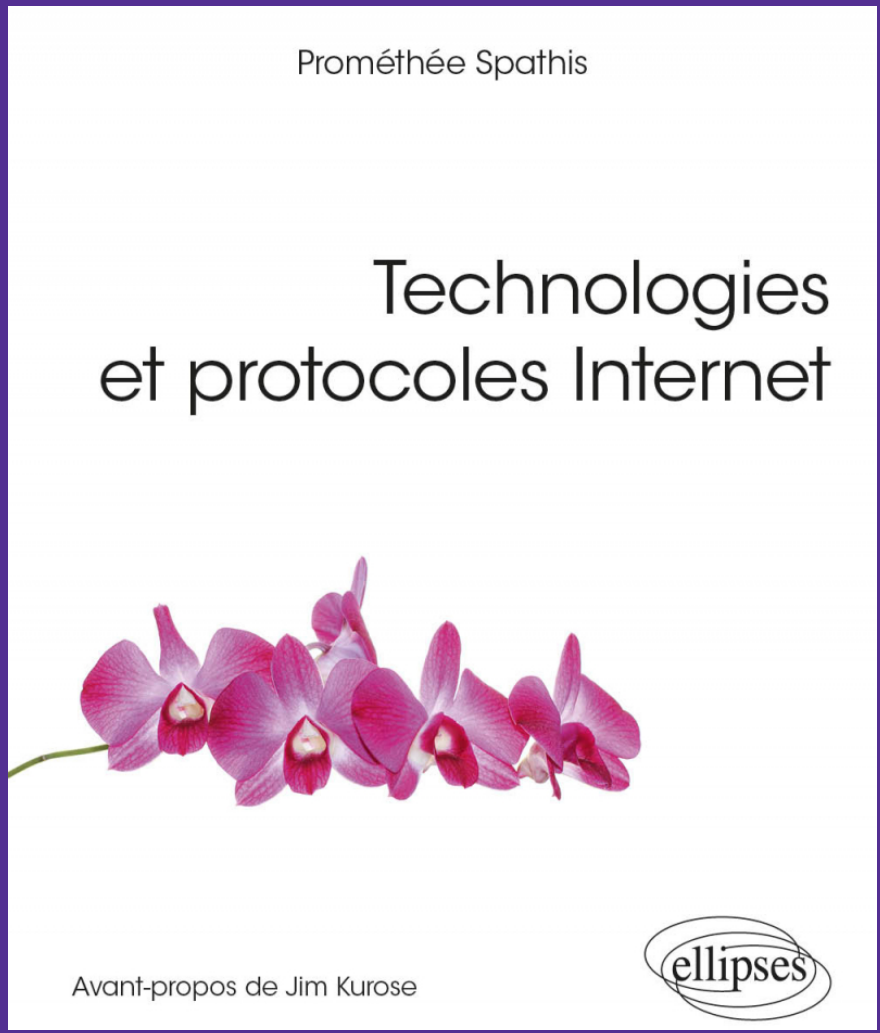
Chap 6 - Paquet IP & ICMP

Ces transparents sont mis à disposition de tous (étudiants, enseignants, lecteurs).

En contrepartie, merci de bien vouloir :

- mentionner leur source,
- préciser la mention de copyright.

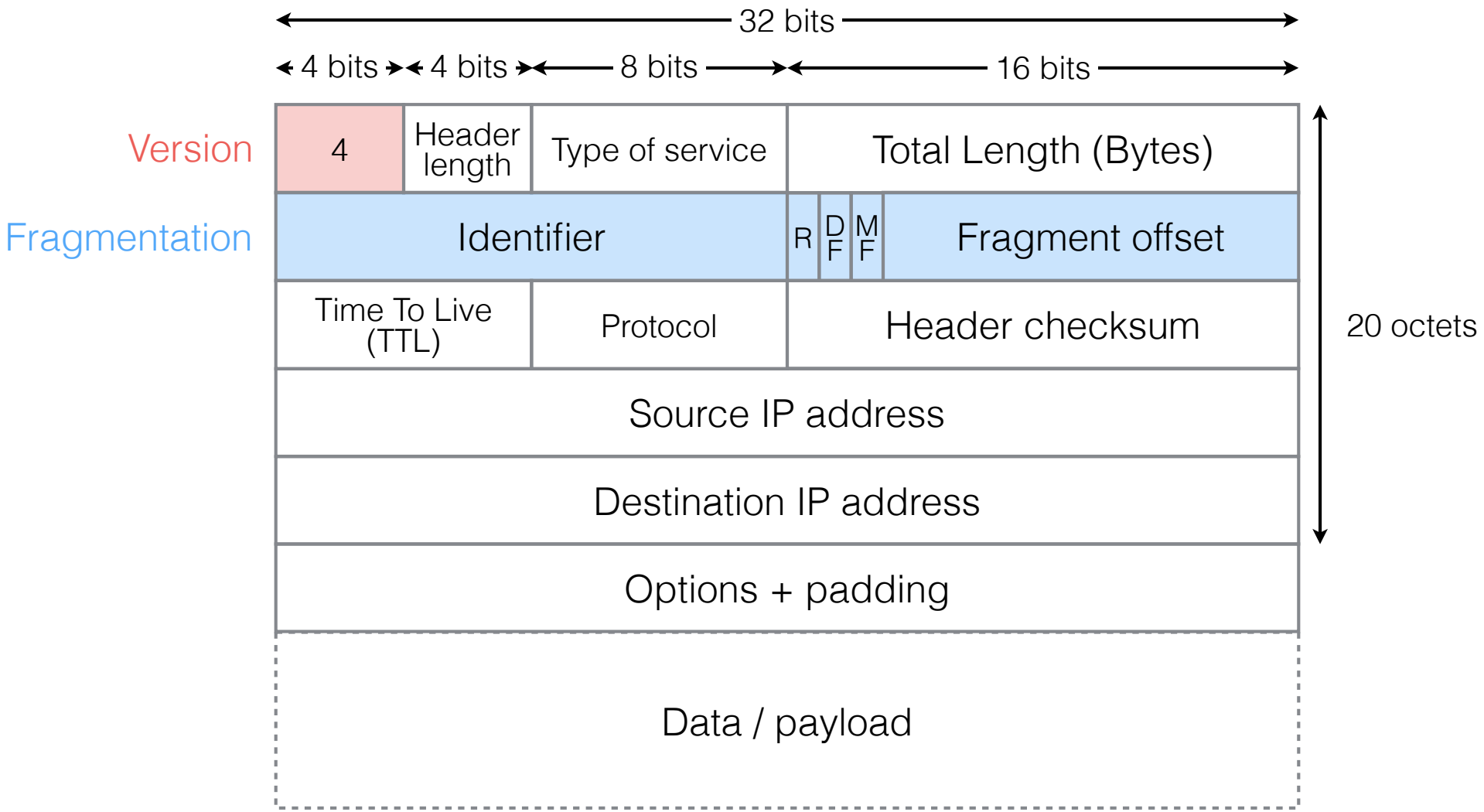
Merci et bon cours !



Plan du cours

- Entête du paquet IPv4
  - Champs de la partie fixe
  - Partie variable : options IP
  - Contrôle d'erreur et boucles de routage
- Longueur d'un paquet IP
  - Taille maximale
  - Fragmentation
- Charge utile du paquet IP
  - Protocoles encapsulés
- Paquet IPv6 et extensions d'entête
- Protocole ICMP
  - Tests et diagnostic d'erreurs
  - ping et traceroute
  - ICMPv6 et Neighbor discovery

Paquet IPv4



Version, Header, ToS

- Version (4 bits)
  - Indique la version du protocole IP
  - Nécessaire pour déterminer la structure de l'entête du paquet
    - Valeurs courantes : "4" (pour IPv4) et "6" (pour IPv6)
- Header length (4 bits)
  - Taille de l'entête exprimée en nombre de mots de 32 bits (4 octets)
    - La valeur "5" (0101) indique une taille de 20 octets (pas d'option IP)
    - La valeur max "15" (1111) indique qu'il y a 40 octets d'options IP
- TOS Type-of-Service (8 bits)
  - Type de chemin sur lequel acheminer le paquet
  - Priorité du paquet par rapport aux autres paquets vus par le routeur
    - Délai faible (transfert audio/video), capacité élevée (téléchargement)

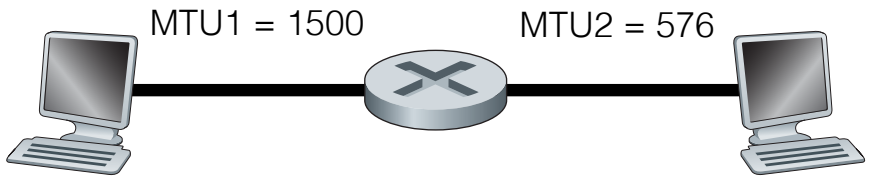
IHL, Fragments, TTL

- Total length (16 bits)
  - Taille totale théorique du paquet exprimée en octets
    - Taille max d'un paquet : 65,535 octets (2^{16} -1)
  - La taille d'un paquet est limitée par la MTU
    - Maximum Transmission Unit MTU : taille max du champ données des trames utilisées par la couche liaison de données sous-jacente
- Fragmentation (32 bits) (voir transparent suivant)
  - Identifiant du paquet, drapeaux, et fragment offset
  - Permet de gérer la fragmentation d'un paquet et le réassemblage des fragments
- Time-To-Live (8 bits)
  - Limite la durée de vie des paquets capturés dans une boucle de routage
  - Correspond au nombre maximal de sauts autorisé du chemin emprunté
  - Valeur décrémentée de 1 par chacun des routeurs que traverse le paquet
  - Suppression du paquet dont le TTL = 0 (ICMP Time exceeded)

Fragmentation IP

MTU Maximum transmission unit : taille max du champ données des trames utilisées par la couche liaison de données sous-jacente

- Flags : 3 bits (Réservé : 0, DF, MF)
  - DF : Don't Fragment (les paquets trop grands sont rejetés)
  - MF : More Fragment (positionné si dernier fragment)
- Fragment Offset :
  - taille en octets hors entête des fragments précédant le fragment courant divisée par 8

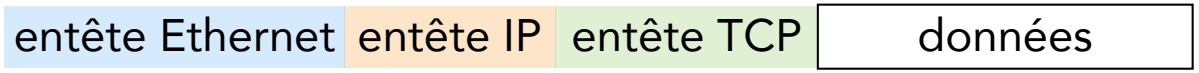


- Exemple :
  - Données encapsulées : 1300 octets
  - Entêtes des fragments sur le réseau 2 :
    - 576 - 20 = 556, valeur multiple de 8 la plus proche : 552 = 69 * 8
    - F1 : offset 0 MF = 1 (taille des données : 552 octets)
    - F2 : offset 69 = 552/8 MF = 1 (taille des données : 552 octets)
    - F3 : offset 69*2 MF = 0 (taille des données : 196 octets)

Protocol, Checksum

- Protocol (8 bits)
  - Identifie le type de l'entête situé après l'entête IP
    - "1" pour ICMP
    - protocoles Transport : "6" pour TCP, "17" UDP
- Checksum (8 bits)
  - Code de détection d'erreurs portant sur l'entête
  - Vérification bout en bout :
    - la source calcule la valeur du checksum
    - le récepteur calcule le checksum sur l'entête reçu et vérifie si la valeur calculée correspond à celle reçue

Exemple : calcul du checksum

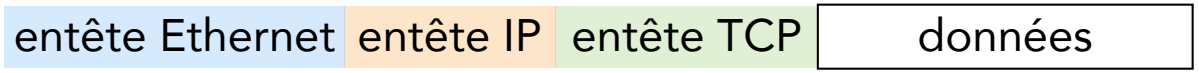



```
08 00 20 87 b0 44 08 00 11 08 c0 63 08 00 45 00
00 48 49 ba 00 00 1e 06 69 8d c1 37 33 f6 c1 37
33 04 17 70 96 d4 39 7f 84 c2 bf 3a 21 fd 50 18
11 1c 99 bc 00 00 0e 00 31 3f 02 c0 00 11 00 00
3e c1 00 00 00 11 00 00 00 02 28 28 a7 b0 80 29
ea fc 81 58 90 70
```

16 bits

```
0x4500      0100 0101 0000 0000
0x0048      0000 0000 0100 1000
            0100 0101 0100 1000
0x49BA      0100 1001 1011 1010
            1000 1111 0000 0010
0x0000      0000 0000 0000 0000
0x1E06      0001 1110 0000 0110
            1010 1101 0000 1000
0x0000      0000 0000 0000 0000
0xC137      1100 0001 0011 0111
          1 0110 1110 0011 1111
0x33F6      0011 0011 1111 0110
          1 1010 0010 0011 0101
0xC137      1100 0001 0011 0111
        10 0110 0011 0110 1100
0x3304      0011 0011 0000 0100
        ---------------------
        10  1001 0110 0111 0000
            1001 0110 0111 0010
0x698D      0110 1001 1000 1101
```

Exemple : vérification du checksum




```
08 00 20 87 b0 44 08 00 11 08 c0 63 08 00 45 00
00 48 49 ba 00 00 1e 06 69 8d c1 37 33 f6 c1 37
33 04 17 70 96 d4 39 7f 84 c2 bf 3a 21 fd 50 18
11 1c 99 bc 00 00 0e 00 31 3f 02 c0 00 11 00 00
3e c1 00 00 00 11 00 00 00 02 28 28 a7 b0 80 29
ea fc 81 58 90 70
```

16 bits

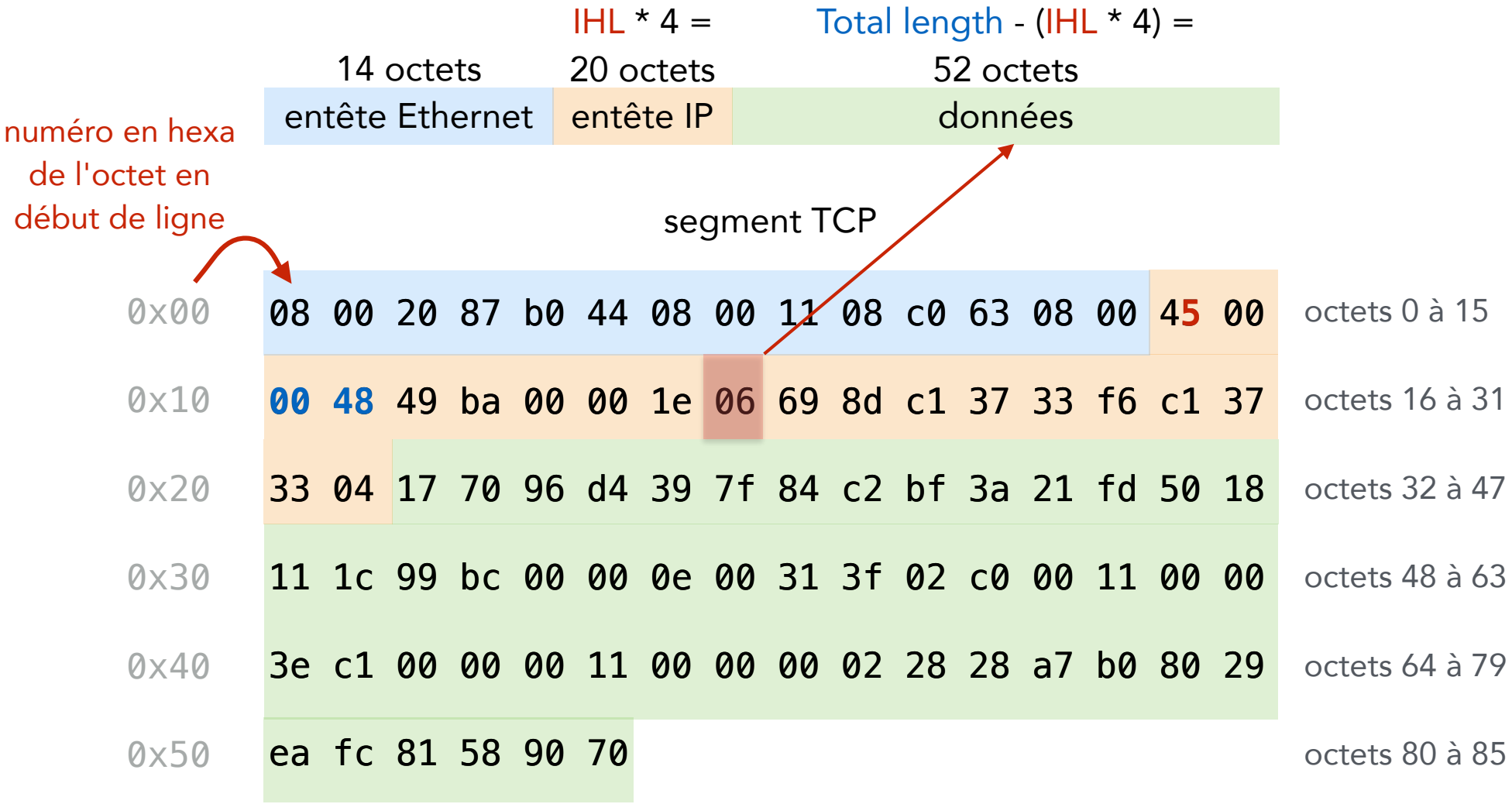
```
0x4500      0100 0101 0000 0000
0x0048      0000 0000 0100 1000
            0100 0101 0100 1000
0x49BA      0100 1001 1011 1010
            1000 1111 0000 0010
0x0000      0000 0000 0000 0000
0x1E06      0001 1110 0000 0110
            1010 1101 0000 1000
0x698D      0110 1001 1000 1101
          1 0001 0110 1001 0101
0xC137      1100 0001 0011 0111
        1 1101 0111 1100 1100
0x33F6      0011 0011 1111 0110
       10 0000 1011 1100 0010
0xC137      1100 0001 0011 0111
       10 1100 1100 1111 1001
0x3304      0011 0011 0000 0100
      ---------------------------
      10 1111 1111 1111 1101
                           10
      ---------------------------
      1111 1111 1111 1111
```

16 bits à 1 : entête sans erreur

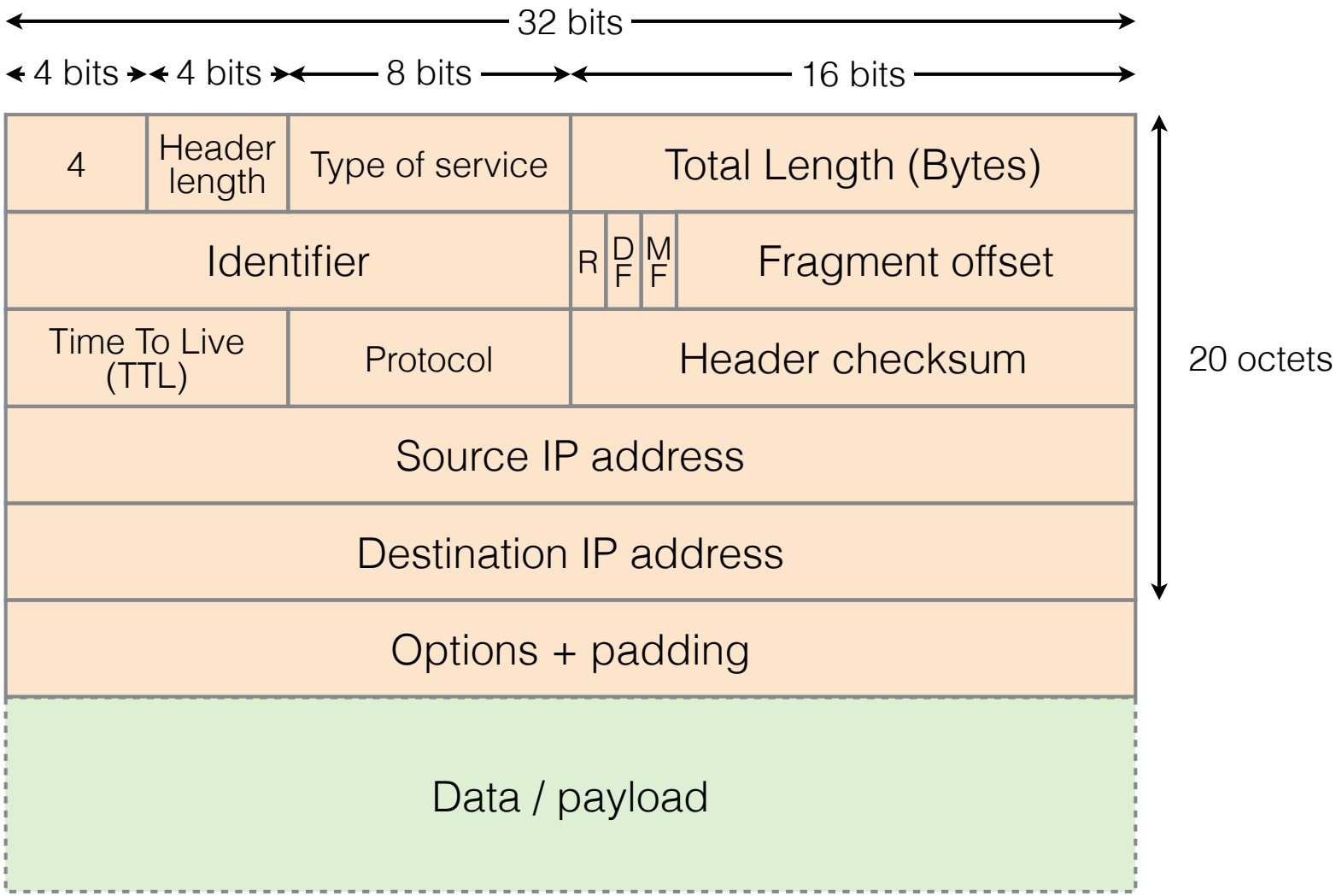
Adresses source et destination

- Deux adresses IP
  - Adresse IP de la source (32 bits)
  - Adresse IP de la destination (32 bits)
- Adresse destination
  - Identifie la machine hôte destination
  - Utilisée par les routeurs pour acheminer le paquet
  - Résulte de la résolution du nom (DNS)
- Adresse source
  - Identifie la machine hôte source
  - Permet à la destination d'accepter ou de rejecter le paquet
  - Utilisée par la destination pour répondre à la source
  - Peut être usurpée
  - Configurée manuellement (administrateur) ou découverte dynamiquement (DHCP)

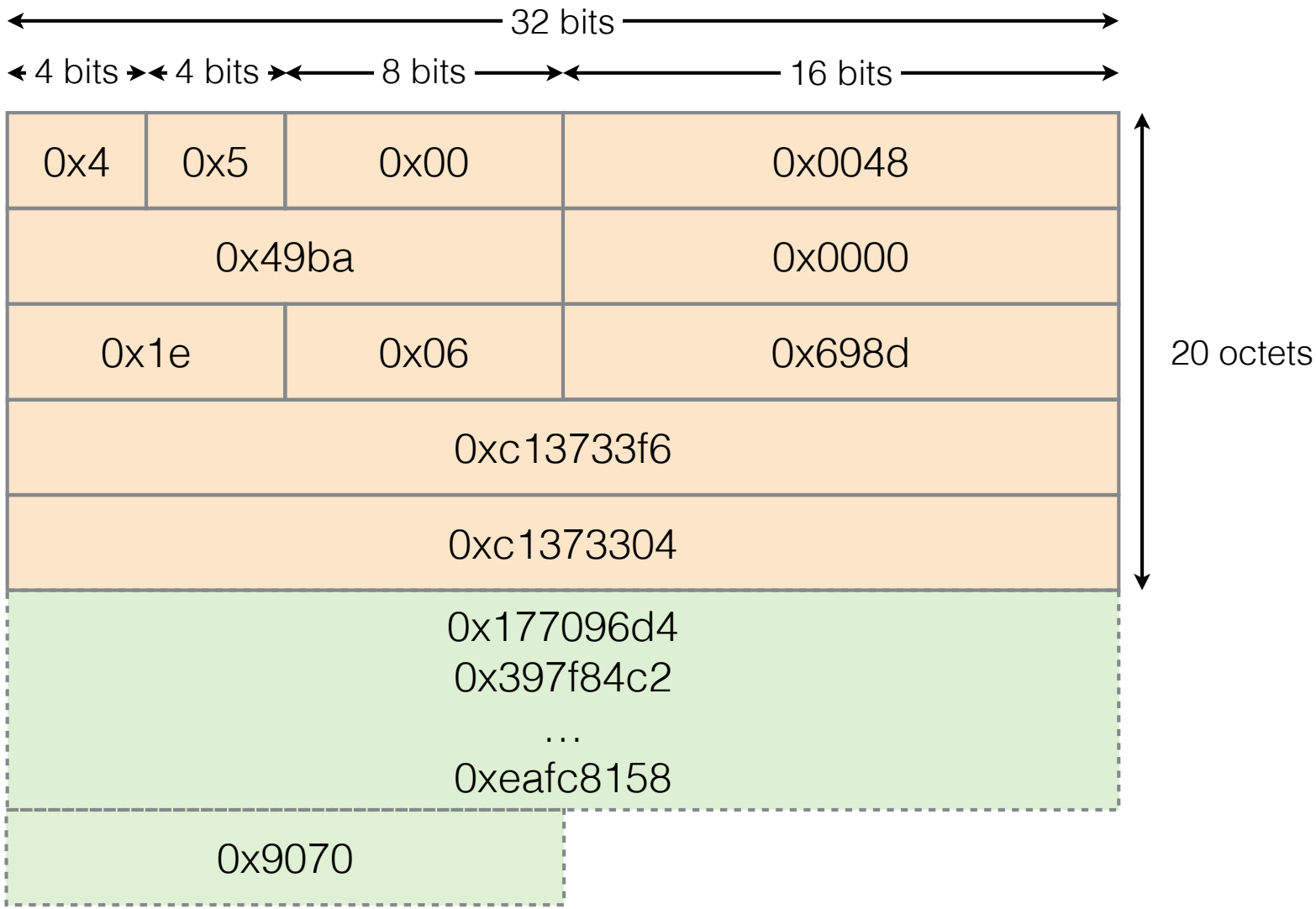
Exemple de trace (1)



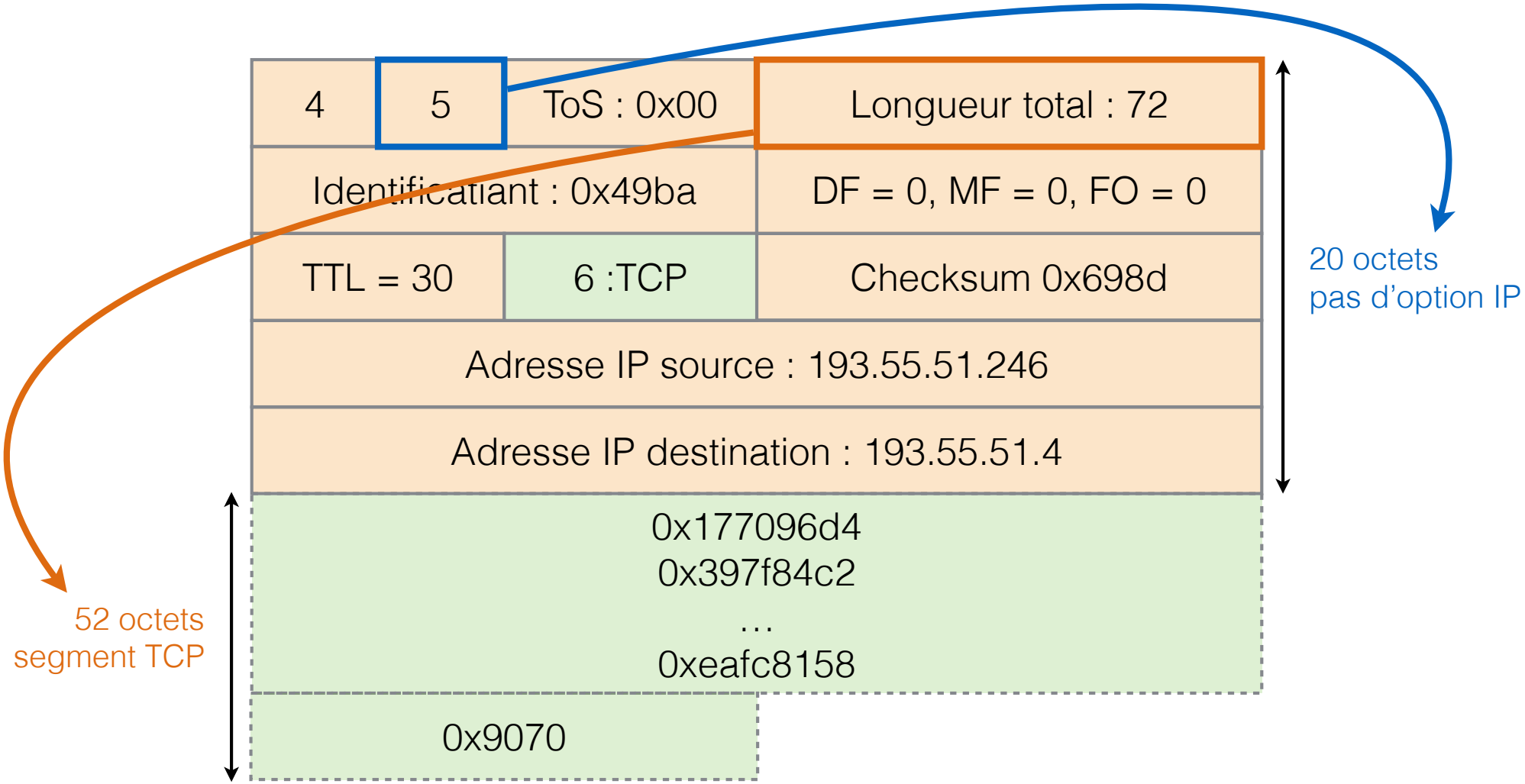
Paquet IPv4



Exemple de trace (2)



Exemple de trace (3)



Exemple de trace (4)

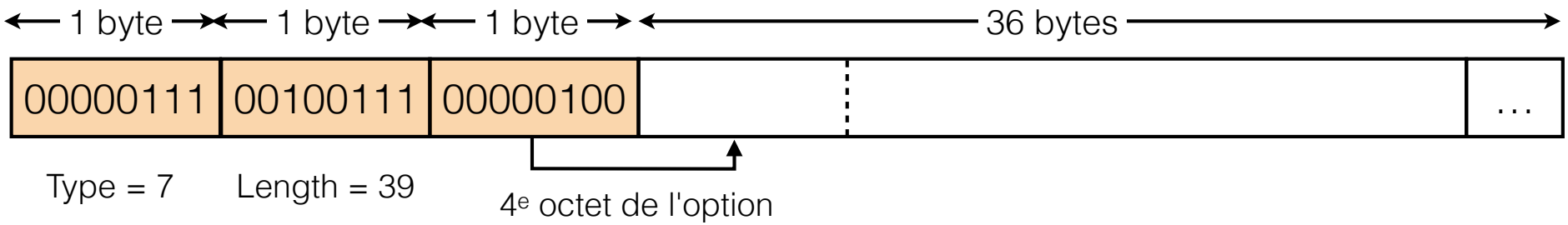
- Version : 0x4 paquet IPv4
- Longueur de l'entête IP : 0x5 20 (5*4) octets
- ToS : 0x00
- Longueur totale : 0x0048 72 octets
- Identifiant : 0x49ba
- DF : 0, MF: 0, Fragment offset : 0
- TTL : 0x1e soit 30 sauts
- Protocole : 0x06 TCP (6)
- Somme de contrôle : 0x698d
- Adresse IP source : 0xc13733f6 soit 193.55.51.246
- Adresse IP destination : 0xc1373304 soit 193.55.51.4
- Données : 72 - 20 = 52 (Longueur totale - Longueur de l'entête)

Options IP

Type	Option	Object
0	End of Options List	Used to coincide the end of the options with the end of the header according to the IHL
1	No Operation	Used to align the beginning of the subsequent option on a 32-bit boundary
7	Record Route (RR)	Used to trace the route an IP packet takes
68	Time Stamp (TS)	Used to records the time (in Universal Time) when each network device receives the packet
131	Loose Routing	Used to route the IP packet based on information supplied by the source
137	Strict Routing	Used to forward the IP packet based on information supplied by the source.

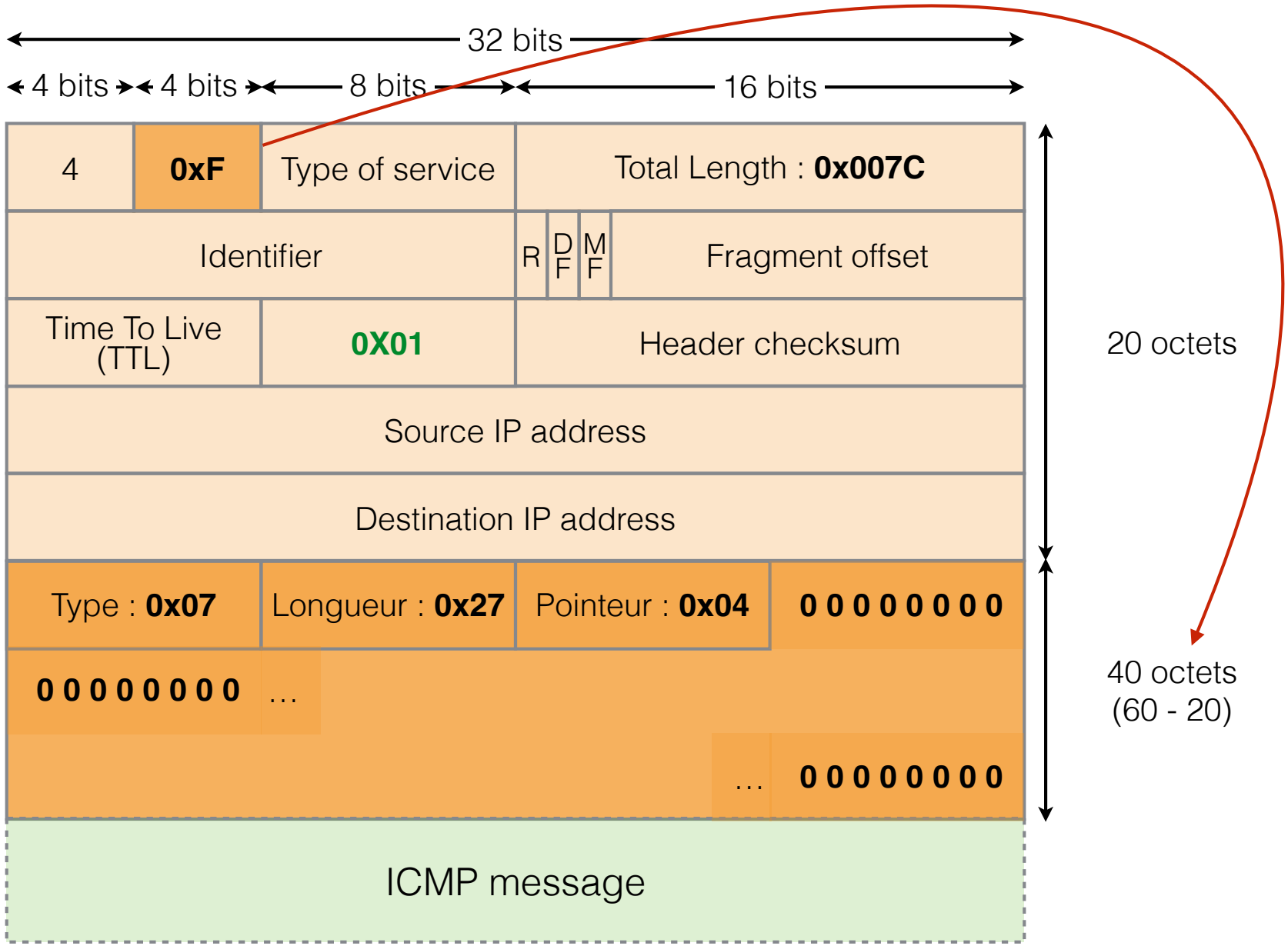
- 131 routage lâche : le paquet IP peut transiter par des routeurs intermédiaires avant d'atteindre le routeur suivant dont l'adresse est spécifiée par l'option
- 137 routage strict : le paquet IP traverse la séquence des seuls routeurs telle que spécifiée par l'option

Option Record Route

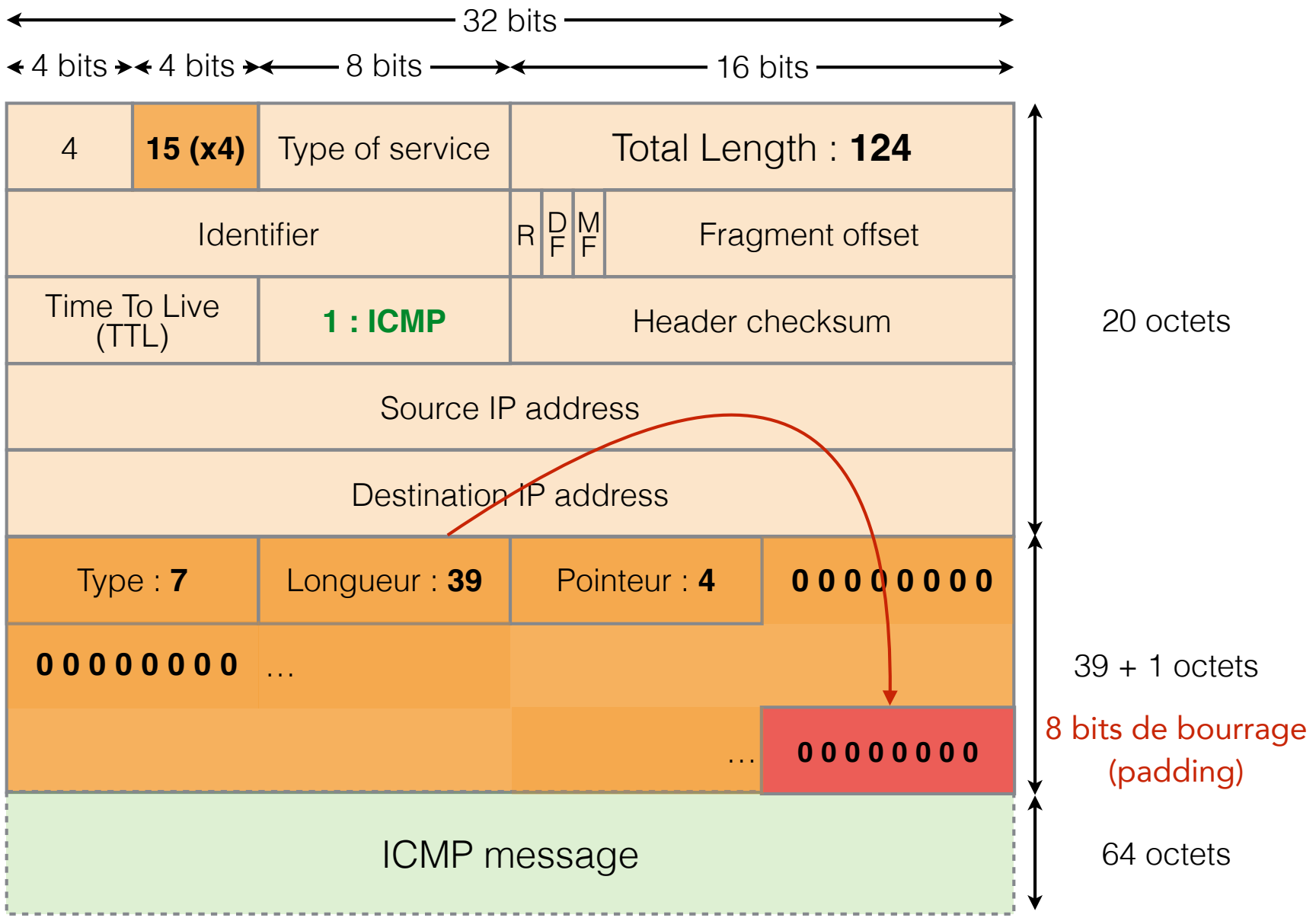



```
08 00 20 0a ac 96 08 00 20 0a 70 66 08 00|4f 00
00 7c cb c9 00 00 ff 01 b9 7f 84 e3 3d 05 c0 21
9f 06 07 27 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 08 00 a2 56 2f 00
00 00 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d
2e 2f 30 31 32 33 34 35 36 37
```

Paquet IPv4 avec option Record Route



Paquet IPv4 avec option Record Route

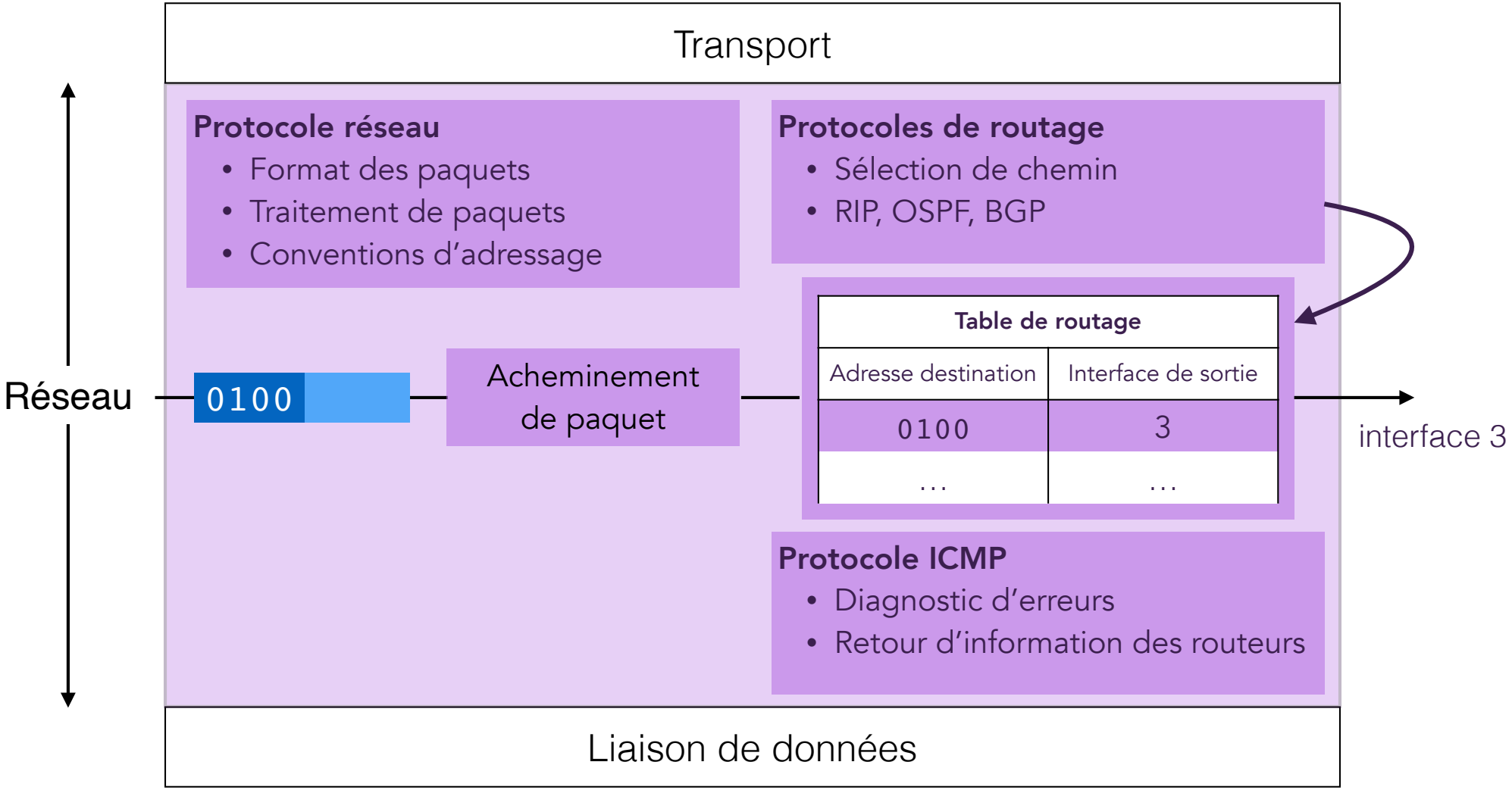


Conclusion

- Champs d'entête du paquet IP
  - les erreurs sur l'entête sont détectées par le checksum
    - les paquets en erreur sont jetés par le récepteur
  - la durée de vie d'un paquet est limitée par son TTL
    - suppression des paquets dont le TTL est nul
- Longueur d'un paquet IP
  - les paquets trop longs peuvent être :
    - fragmentés avant d'être acheminés sur une liaison avec une MTU restrictive
    - supprimés par ces même routeurs
- Charge utile du paquet IP
  - le type de l'entête encapsulé par un paquet est identifié par le champ Protocole
    - 6 : TCP, 17 : UDP, 1 : ICMP

Le protocole ICMP

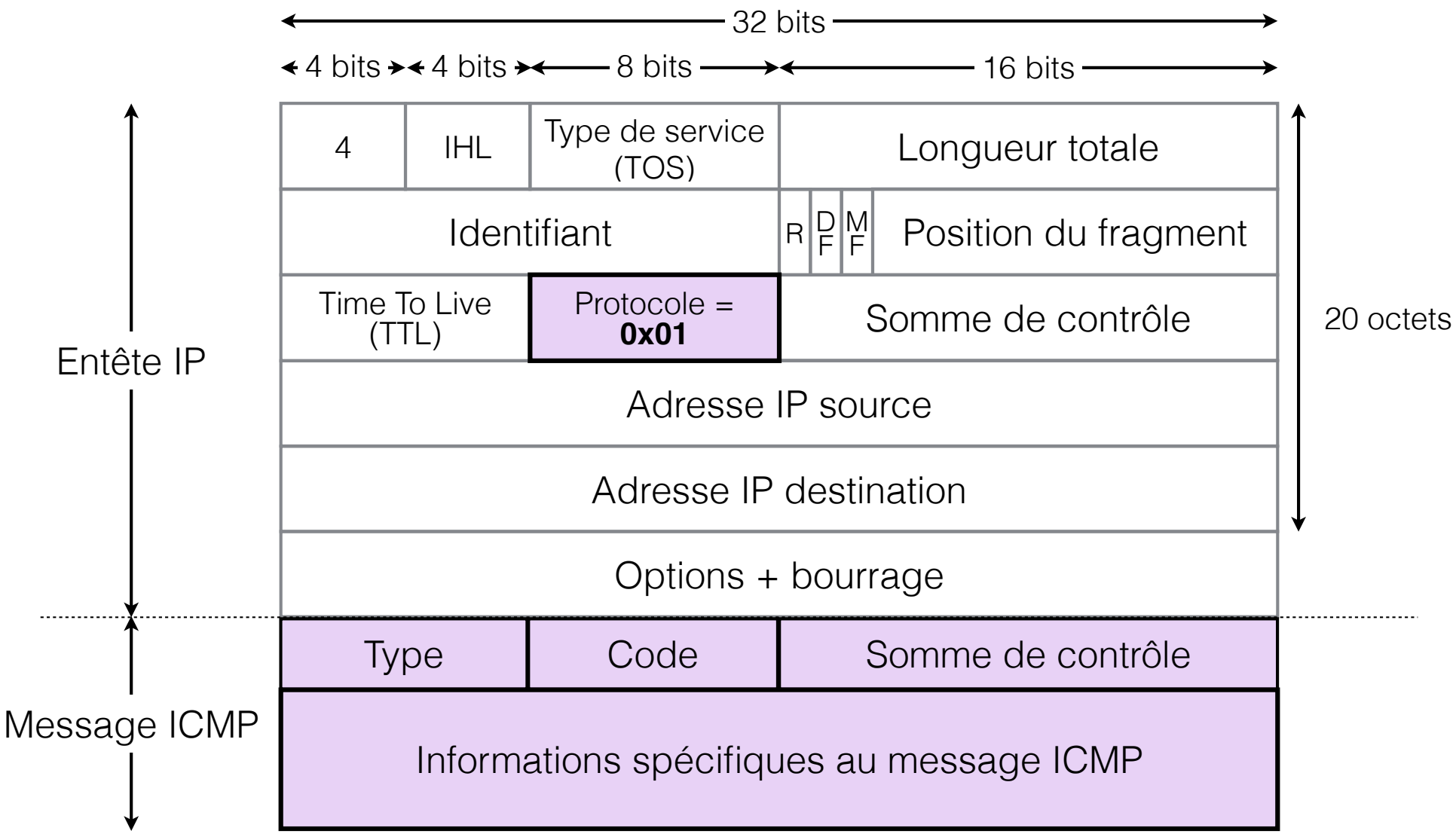
Protocole ICMP



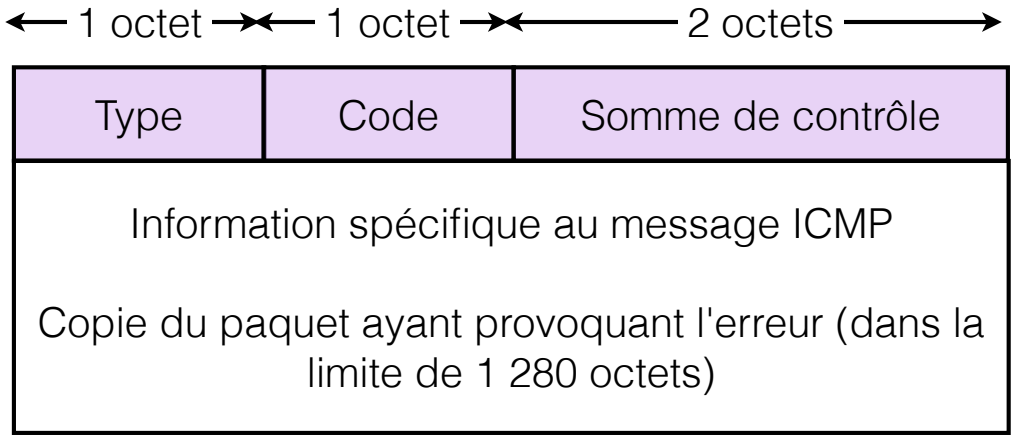
Protocole ICMP

- Fonctionnalités de ICMP :
  - messages d'erreur en cas d'erreurs d'acheminement ou de livraison
  - messages d'information permettant des tests de connectivité
- Implémenté au dessus d'IP
  - au même niveau que TCP (6) ou UDP (17)
  - champ Protocol IP : 1
- Diagnostics d'erreur
  - messages ICMP retournés à la source en cas de problème
  - temps dépassé, paquet trop grand, destination inaccessible, …
- Les messages ICMP contiennent :
  - des informations relatives à l'erreur
    - type : nature de l'erreur, code : raison de l'erreur
  - copie partielle du paquet ayant provoqué l'erreur (dans la limite de 1480 octets)

Encapsulation IP de ICMP



ICMP Messages

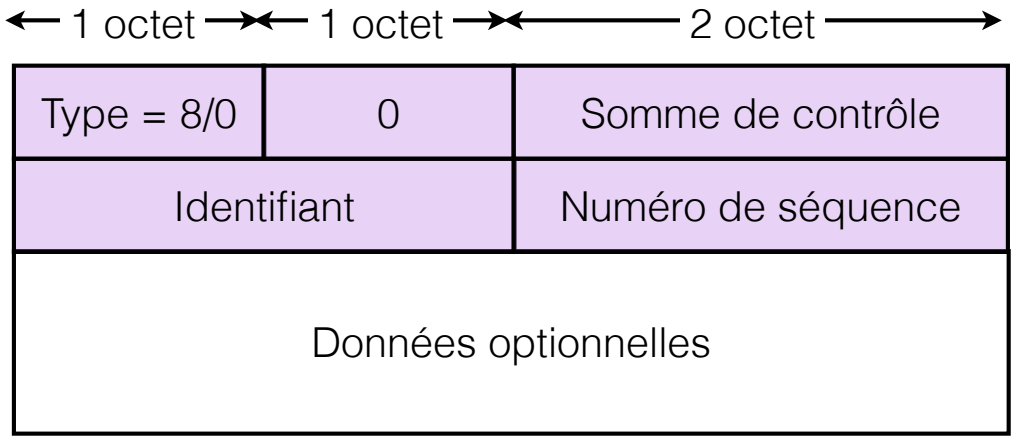


- Type: nature du message ICMP
  - messages d'erreur
  - messages d'information
- Code: cause de l'erreur
- Somme de contrôle (checksum) :
  - Vérification de l'intégrité :
    - du message ICMP
    - du pseudo-entête IP (similaire à TCP et UDP)

Types et codes ICMP

Type	Code	Message
0	0	Echo Reply
3	0	Destination Network Unreachable
3	1	Destination Host Unreachable
3	2	Destination Protocol Unreachable
3	3	Destination Port Unreachable
3	6	Destination Network Unknown
3	7	Destination Host Unknown
4	0	Source Quench
5	0	Redirect
8	0	Echo Request
11	0	Time Exceeded
11	1	Reassembly Time Exceeded
12		Parameter Problem
13		Timestamp
14		Timestamp Reply
15		Information Request
16		Information Reply
17		Address Mask Request
18		Address Mask Reply

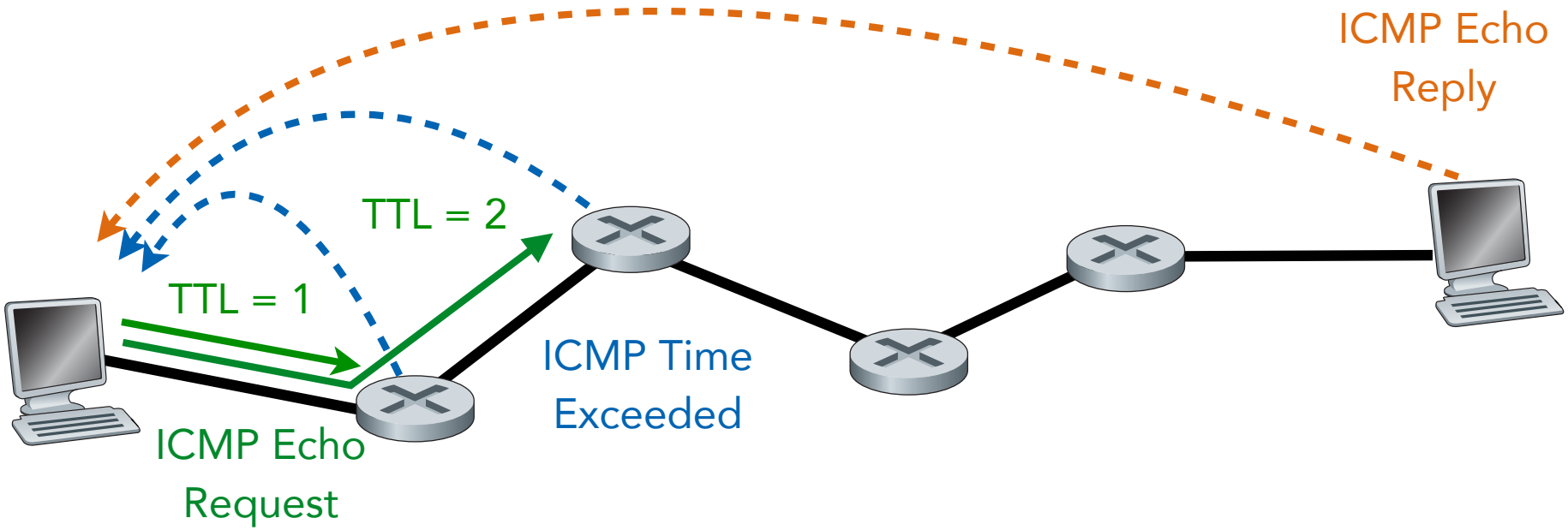
Echo Request (Type=8) / Echo Reply (Type=0)



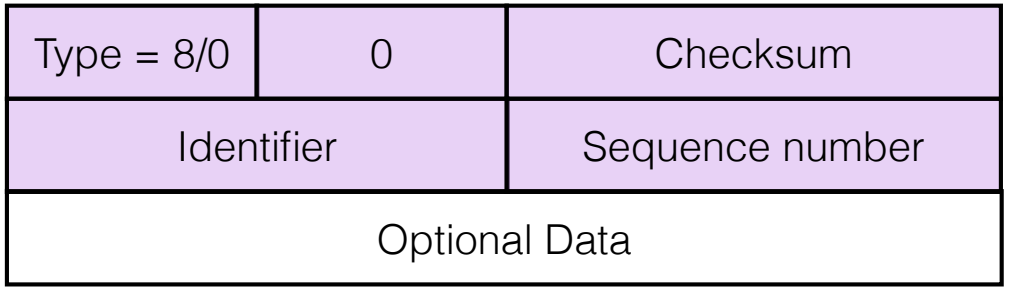
- Pour vérifier si une machine est joignable ou les problèmes de routage
  - mesure du délai aller-retour (valeurs min max moyenne)
  - comptage des messages Echo request ou Echo reply perdus
- Champ Identifier :
  - permet de faire correspondre les messages Echo Reply reçus aux messages Echo Request si envoyés à différentes machines
- Champ Sequence Number :
  - permet de faire correspondre un Echo Reply à l'Echo request correspondant si plusieurs Echo Request envoyés à la même machine

Traceroute

- La commande Traceroute envoie des messages ICMP 'Echo Request' en incrémentant leur TTL

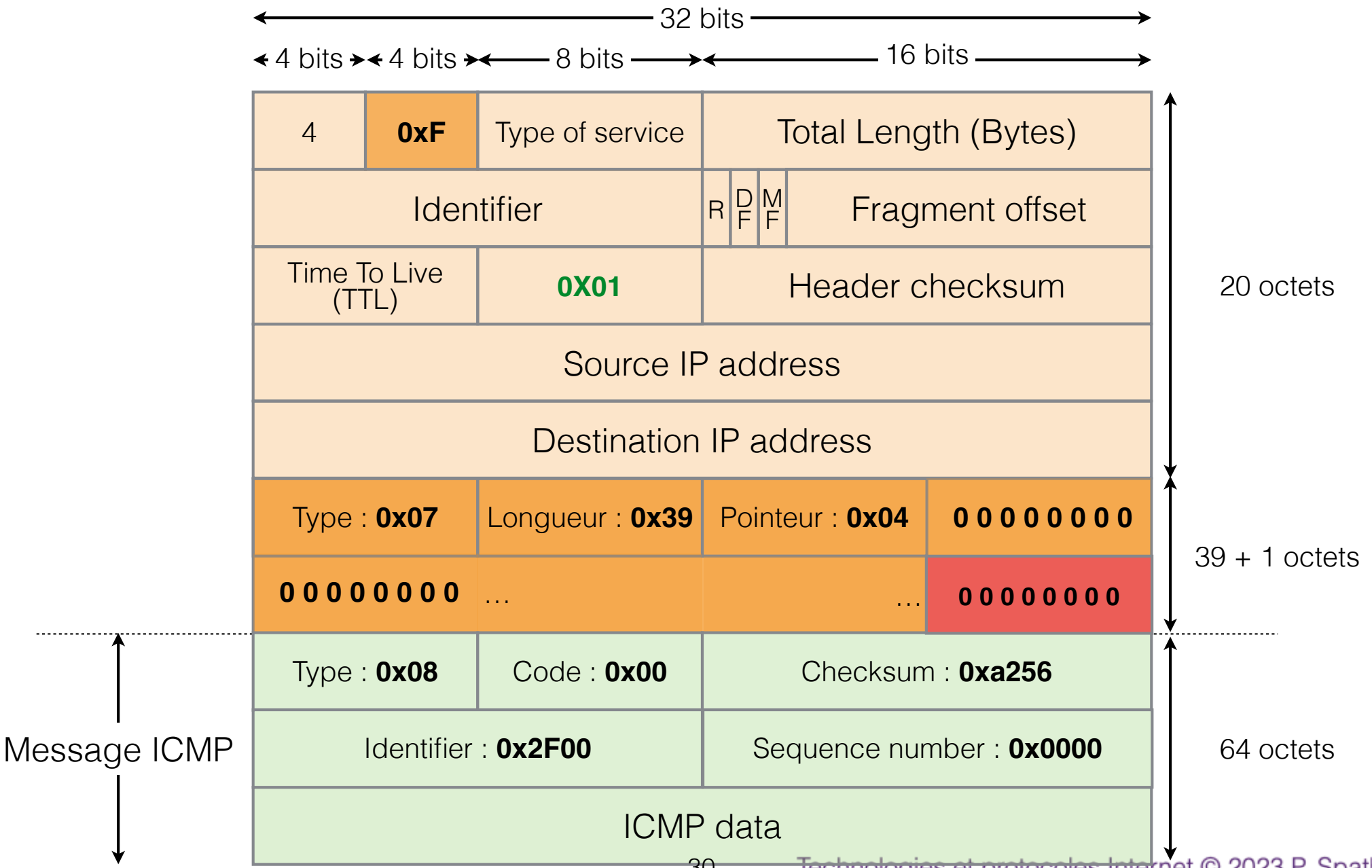


Option Record Route




```
08 00 20 0a ac 96 08 00 20 0a 70 66 08 00|4f 00
00 7c cb c9 00 00 ff 01 b9 7f 84 e3 3d 05 c0 21
9f 06 07 27 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 08 00 a2 56 2f 00
00 00 29 36 8c 41 00 03 86 2b 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d
2e 2f 30 31 32 33 34 35 36 37
```

Paquet IPv4 avec option Record Route

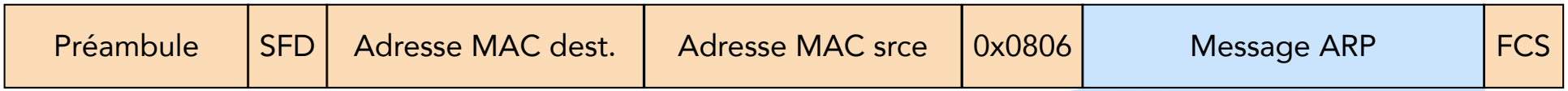


ARP
Découverte des adresses MAC des machines voisines

Address Resolution Protocol (ARP)

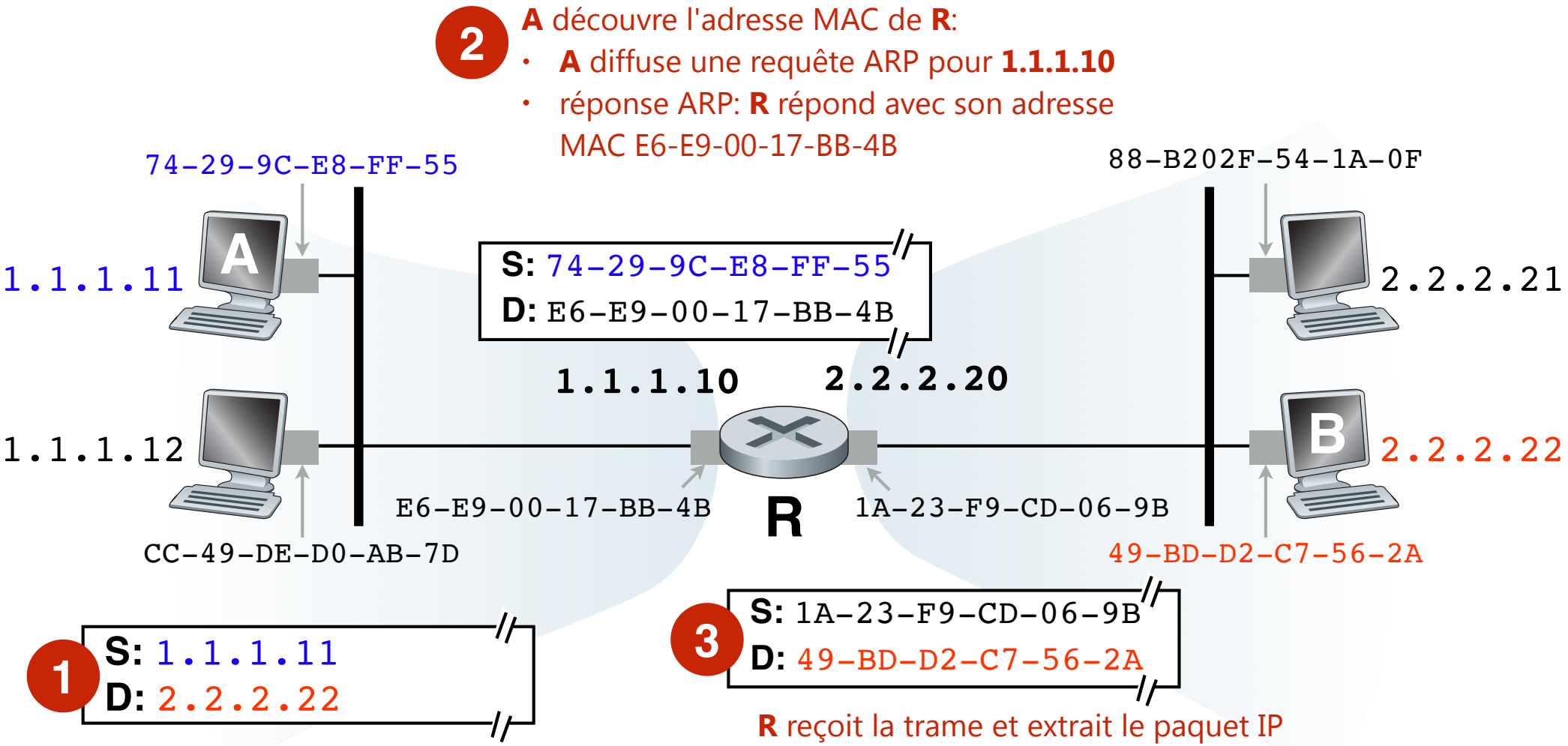
- Les machines hôtes maintiennent une table ARP :
  - Une correspondance (IP adresse, MAC adresse) par entrée
  - Entrées configurées manuellement ou découvertes par envoi de requêtes ARP
  - Les correspondances découvertes expirent à l'issue d'un temporisateur
- Une machine hôte qui souhaite envoyer un paquet IP consulte sa table ARP :
  - Si une entrée est trouvée pour l'adresse IP destination du paquet :
    - Encapsuler le paquet IP dans une trame destinée à l'adresse MAC spécifiée par cette entrée
  - Sinon :
    - Diffuser une requête ARP contenant l'adresse IP à résoudre
    - La cible retourne une réponse ARP contenant son adresse MAC
    - Encapsuler le paquet IP dans une trame destinée à l'adresse MAC retournée
    - Créer une nouvelle entrée dans la table ARP pour cette cible

Format des messages ARP



- Protocol Type
  - IPv4 = 0x0800
- Hardware Type
  - Ethernet = 1
  - HDLC = 17
- HLEN (longueur adresse physique)
  - Ethernet = 48
- PLEN (longueur adresse logique)
  - IPv4 = 32
- Operations
  - Requête ARP = 1
  - Réponse ARP = 2

Hardware type		Protocol type
HLEN (n)	PLEN (m)	Operations
Source Hardware Address: n		
Source Protocol Address: m		
Destination Hardware Address: n		
Destination Protocol Address: m		

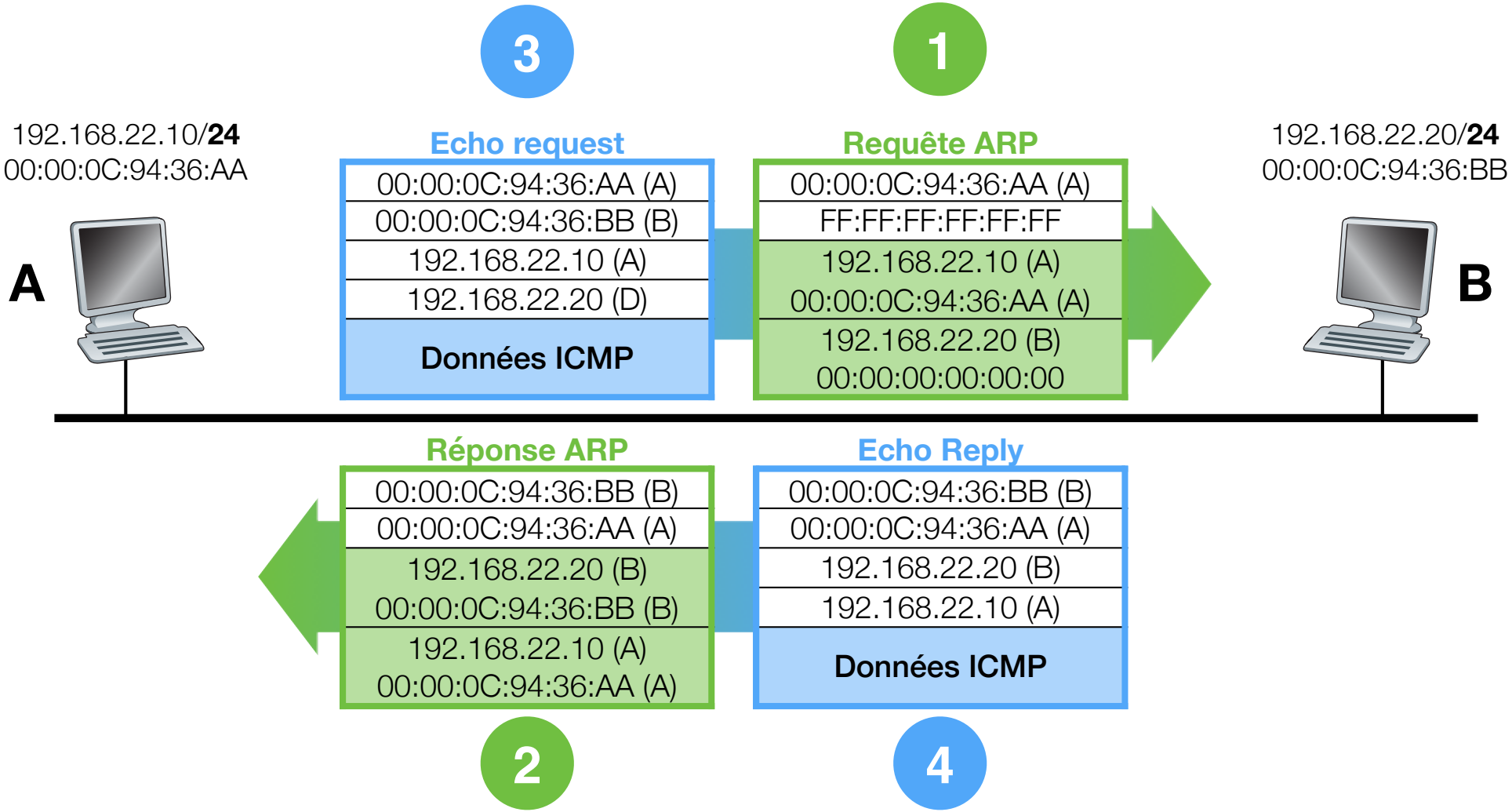


A désire envoyer un paquet à **B**
Les préfixes de **A** et **B** sont différents
A doit envoyer son paquet à la gateway **R**
(acheminement indirect)

R reçoit la trame et extrait le paquet IP
R cherche dans sa table de routage l'interface sortante pour 2.2.2.22
R diffuse une requête ARP pour 2.2.2.22
B répond avec l'adresse MAC 49-BD-D2-C7-56-2A
R encapsule le paquet dans une trame qu'il envoie à **B**

On suppose les tables ARP de A et R vides

ARP & ICMP

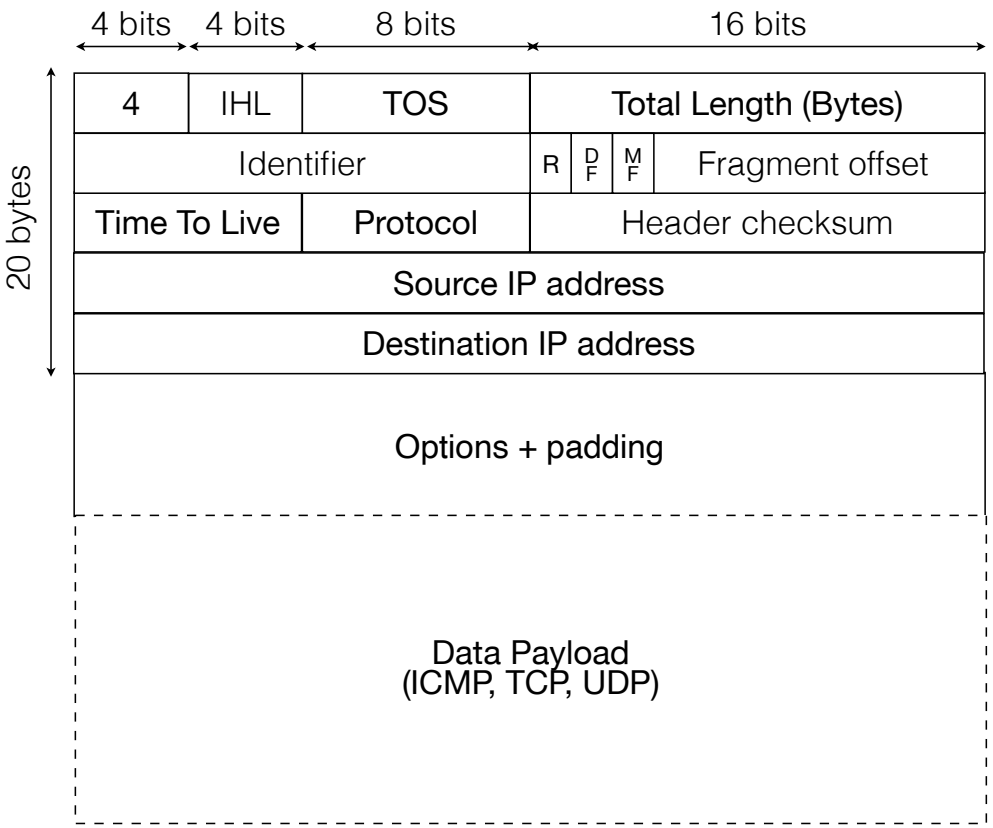


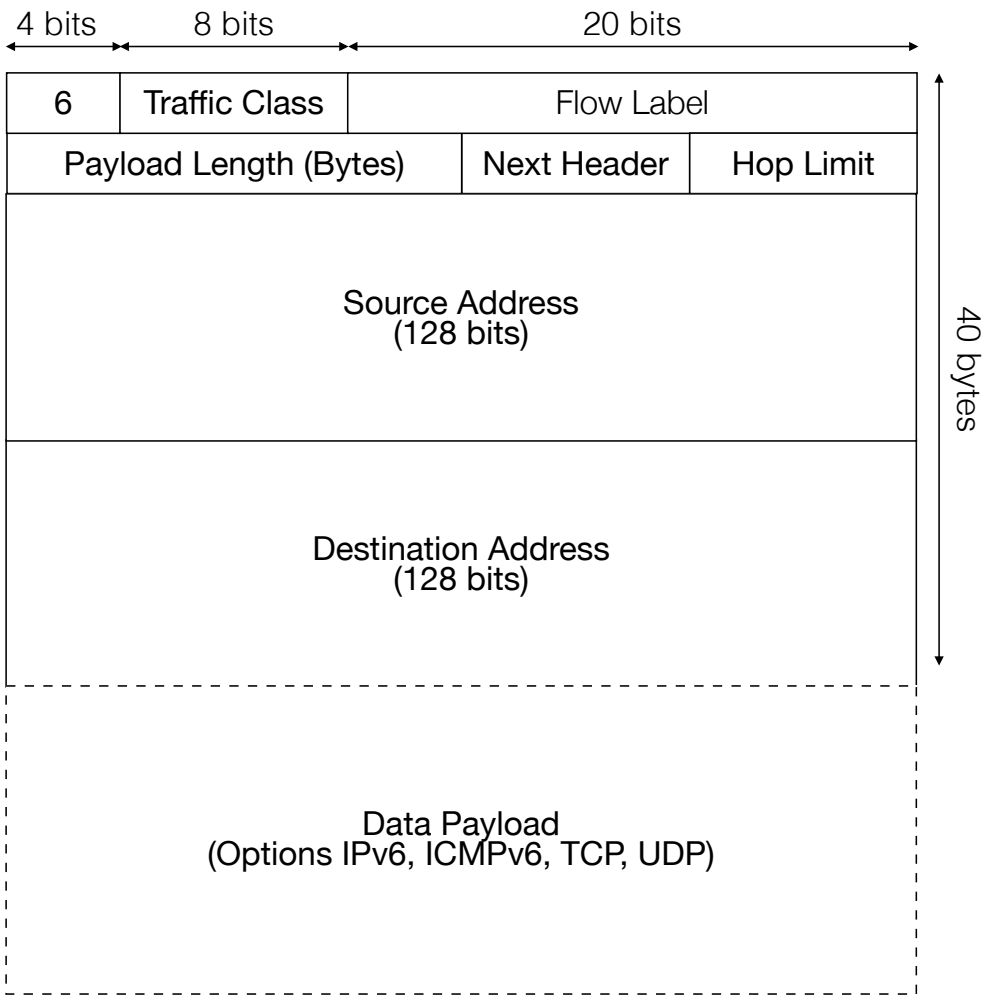
Paquet IPv6

Différences notables entre IPv4 et IPv6

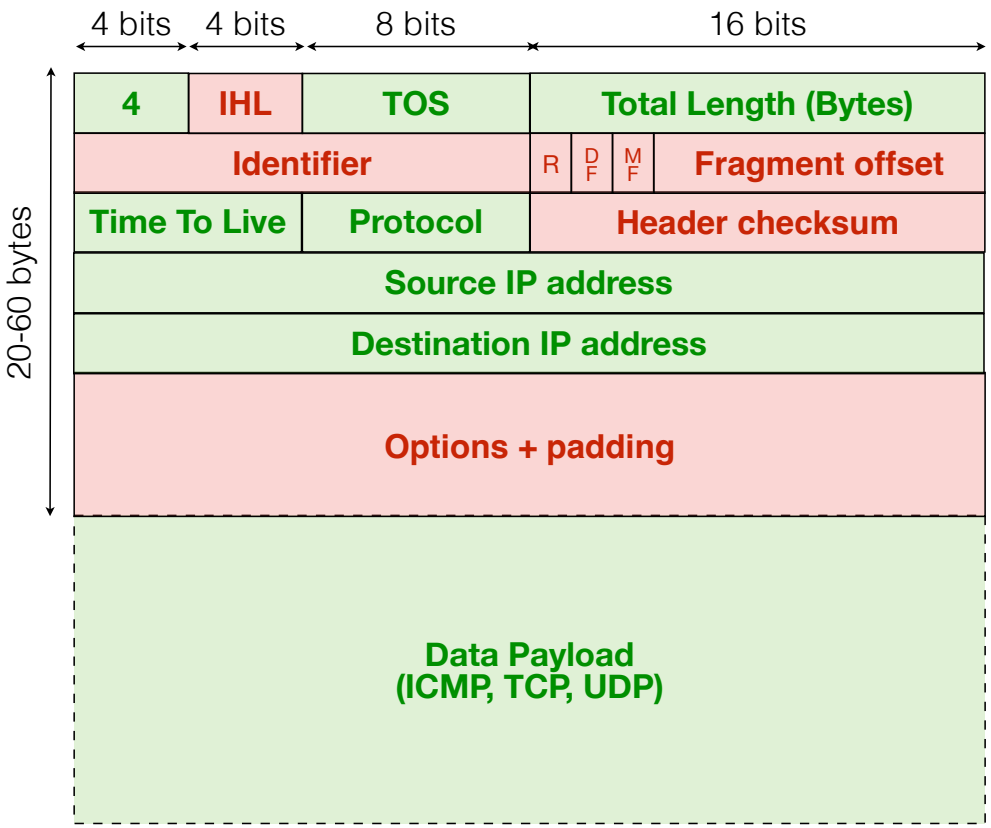
- Les adresses IPv6 sont longues de 128 bits
  - Les classes IPv4 classes sont remplacées par different types d'adresses IPv6
  - Notation hexadécimale double pointée avec longueur de préfixe (CIDR) :
    - FF01:0000:0000:0000:0000:0000:0000:0043/8
  - Format compressé : FF01::43/8 (FF01:~~0000:0000:0000:0000:0000:0000:00~~43/8)
- L'entête IPv6 est deux fois plus long qu'IPv4 pour un nombre de champs réduit de moitié
  - L'entête IPv6 est long de 40 octets et est aligné sur de mots de 64 bits
  - Les options IPv6 sont implémentées sous forme d'extension d'entête
    - de nouvelles valeurs ont été ajoutées au champ *Protocol* (renommé champ *Next Header* dans IPv6)
- ICMPv6 est la nouvelle version de ICMP et comprend des messages supplémentaires
  - Messages NDP (Neighbor Discovery Protocol)
    - en remplacement de ARP, des messages ICMP Route Redirect et ICMP Router Discovery
  - Messages MLD (Multicast Listeners Discovery) and MRD (Multicast Router Discovery)
    - en remplacement de IGMP

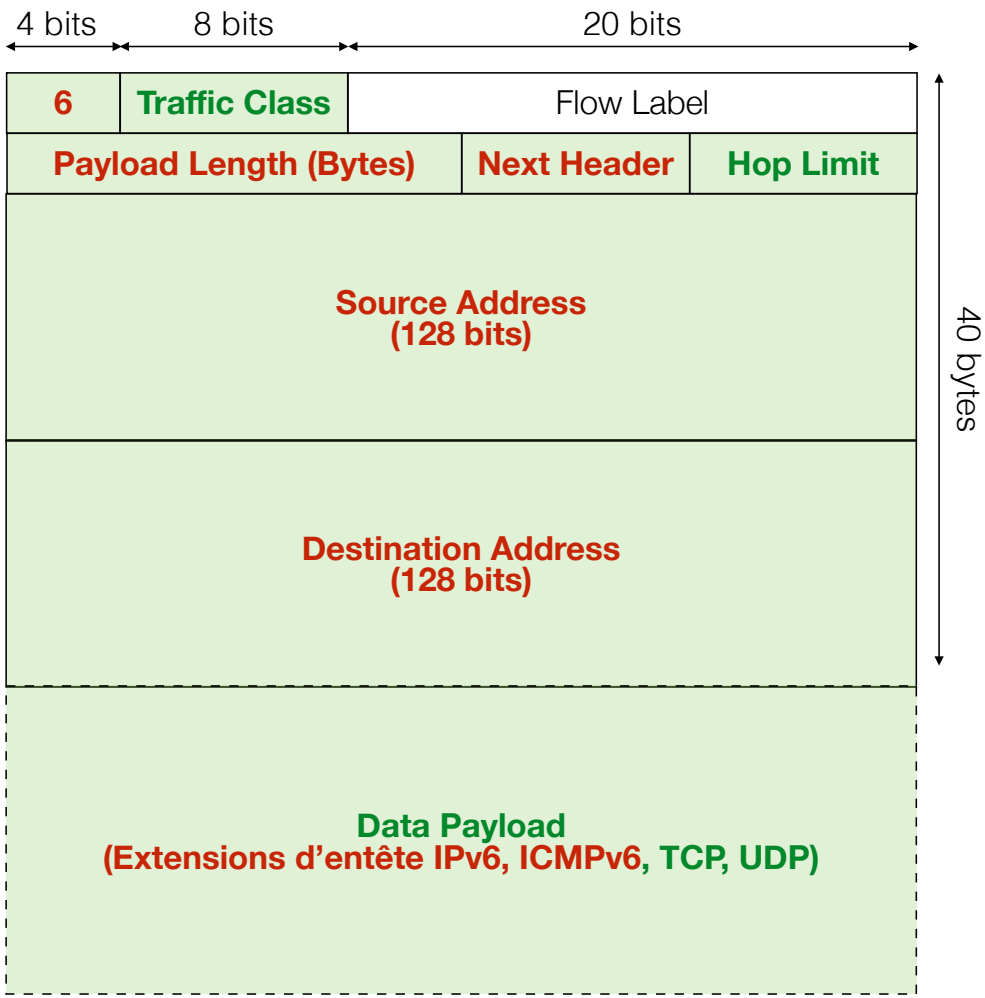
Entête IPv4 vs IPv6





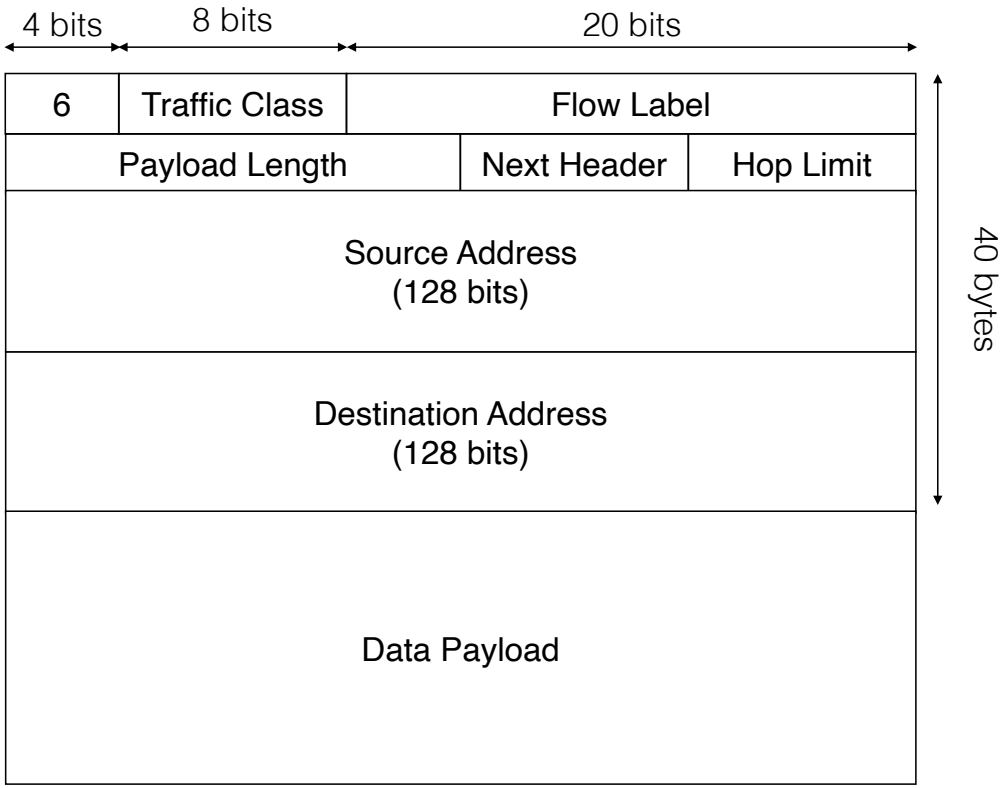
Entête IPv4 vs IPv6



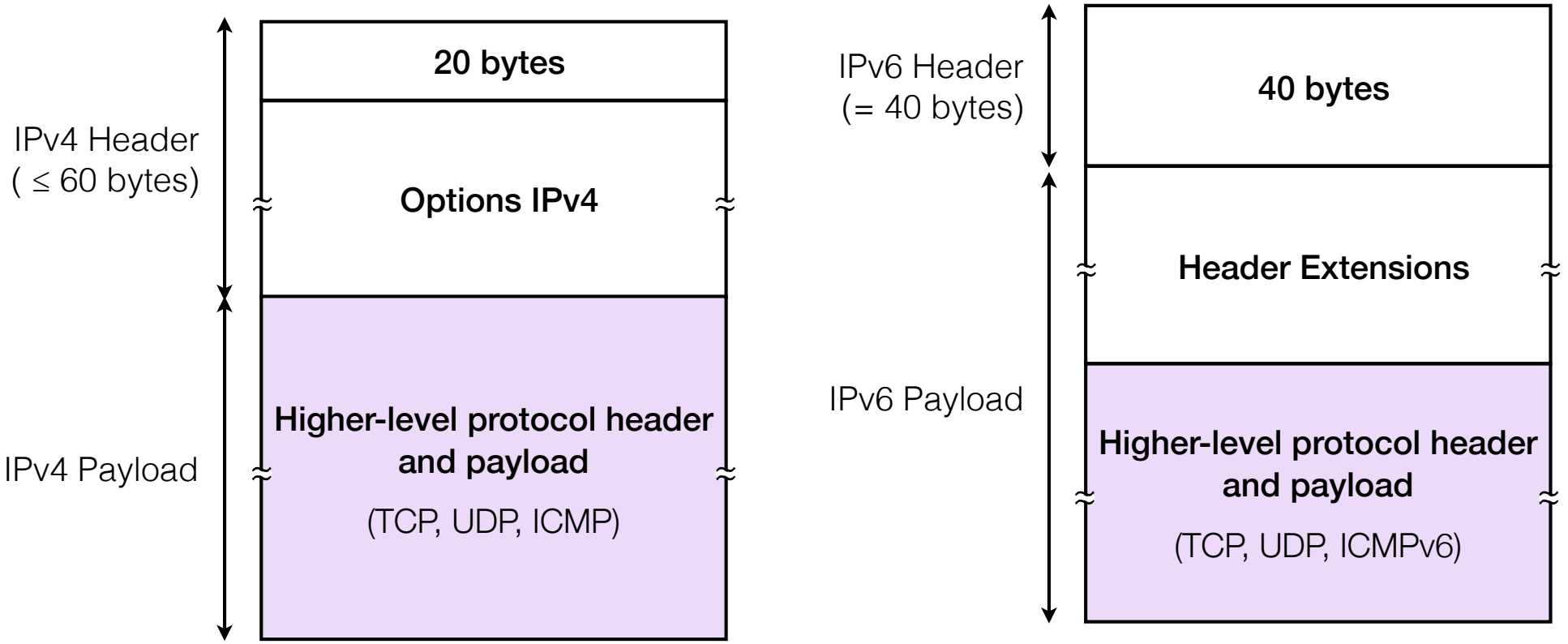


Entête IPV6

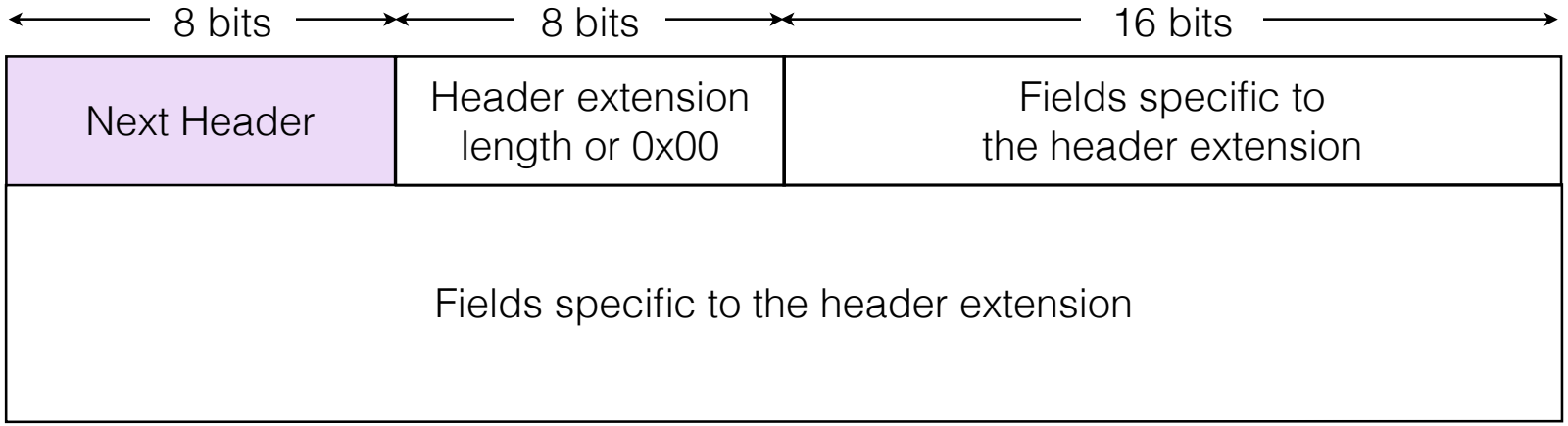
- Version: 4 → 6
- Header Length (IHL): retiré
- ToS → Traffic Class
- Total Length → Payload Length
- ID, Flags et Fragment Offset (FO): retiré
  - prise en charge par l'extension d'entête Fragment
- TTL → Hop Limit
- Protocol → Next header
  - valeurs identiques à IPv4, ajout des valeurs pour les Extensions d'entête
- Header Checksum: retiré
  - pseudo-entête requis pour ICMPv6 et les protocoles de la couche transport
- Adresses : 32 → 128 bits (4 → 16 octets)
- Alignment sur des mots de 32 bits → 64 bits



IPv4 Options vs IPv6 Header Extensions

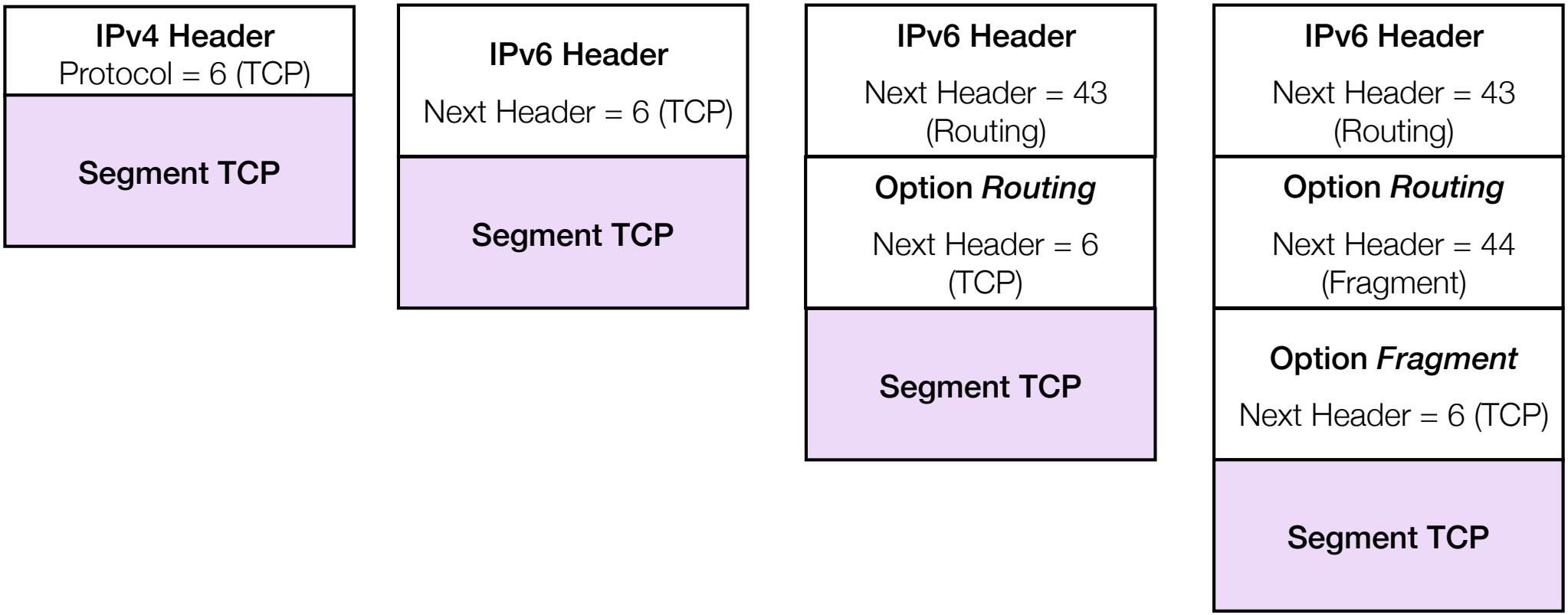


Extension d'entête IPv6



- Alignement des Extensions d'entête sur des mots de 8-octets
- Une Extension d'entête contient :
  - Le champ Next Header
  - La longueur de l'extension d'entête sur 8 bits :
    - 0x00 si l'extension d'entête est longue de 8 octets
    - Le nombre de mots de 8 octets sans inclure le premier mot de 8 octet
  - Les champs spécifiques à l'extension d'entête

IPv4 Options vs IPv6 Header Extensions



Protocole ICMPv6

ICMPv6

- ICMPv6 inclut les messages IPv4 ICMP de reporting et de diagnostic
  - erreurs de livraison et de forwarding
    - destination unreachable, time exceed, packet too big, …
  - service d'echo pour diagnostic
    - echo request/reply (ping)
- ICMPv6 comprend de nouveaux types de message (Type ≥ 127)
  - Neighbor Discovery (ND)
    - inclut 5 messages pour communiquer avec ses voisins directs
    - remplace ARP, les messages ICMPv4 Redirect et Router Discovery
  - Multicast Listener Discovery (MLD)
    - inclut 3 messages
    - similaire à IGMP

Neighbor Discovery

- ND est utilisé par les machines hôtes pour :
  - découvrir les routeurs voisins
  - découvrir les addresses, les préfixes et autres paramètres de configuration
- ND est utilisé par les routeurs pour :
  - annoncer leur présence, les préfixes du réseau local, les paramètres de configuration
  - informer les machines hôtes de l'adresse d'un meilleur saut suivant pour acheminer les paquets étant donné une destination
- ND est utilisé par un nœud (hôte ou routeur) pour :
  - résoudre l'adresse physique d'un nœud voisin
  - déterminer si un voisin est toujours joignable
- ND utilise le multicast pour certains de ses services

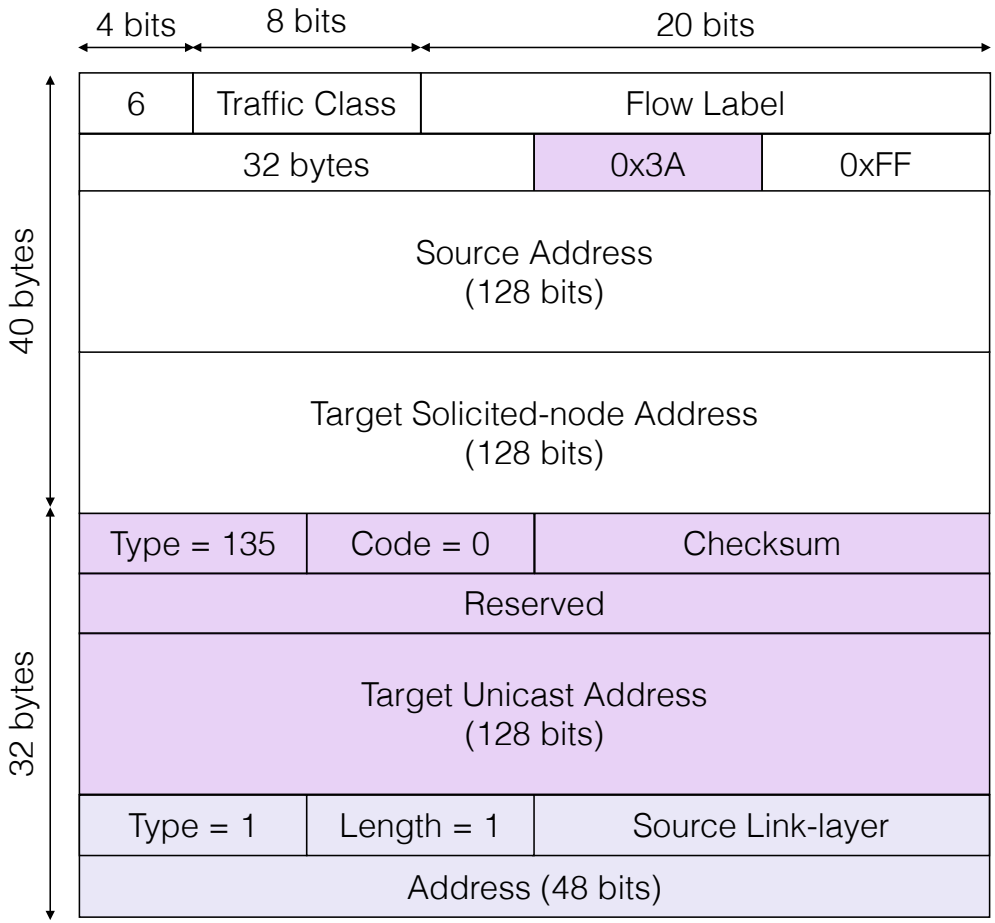
Les types de messages ND

- Router Advertisement (RA) :
  - annonce périodique (la disponibilité d'un routeur) qui contient :
    - la liste des préfixes utilisés sur le lien local (autoconf)
    - la valeur par défaut du Max Hop Limit
    - la valeur de la MTU
- Router Solicitation (RS) :
  - sollicitation envoyée par un hôte pour recevoir un RA immédiatement (à son démarrage)
- Neighbor Solicitation (NS):
  - détermine l'adresse physique d'un voisin
  - vérifie la disponibilité d'un voisin
  - vérifie si une adresse est dupliquée sur le lien local (DAD)
- Neighbor Advertisement (NA):
  - en réponse à un message NS
  - pour annoncer le changement de son adresse physique
- Redirect :
  - utilisé par un routeur pour informer un hôte d'un meilleur saut suivant étant donné une destination

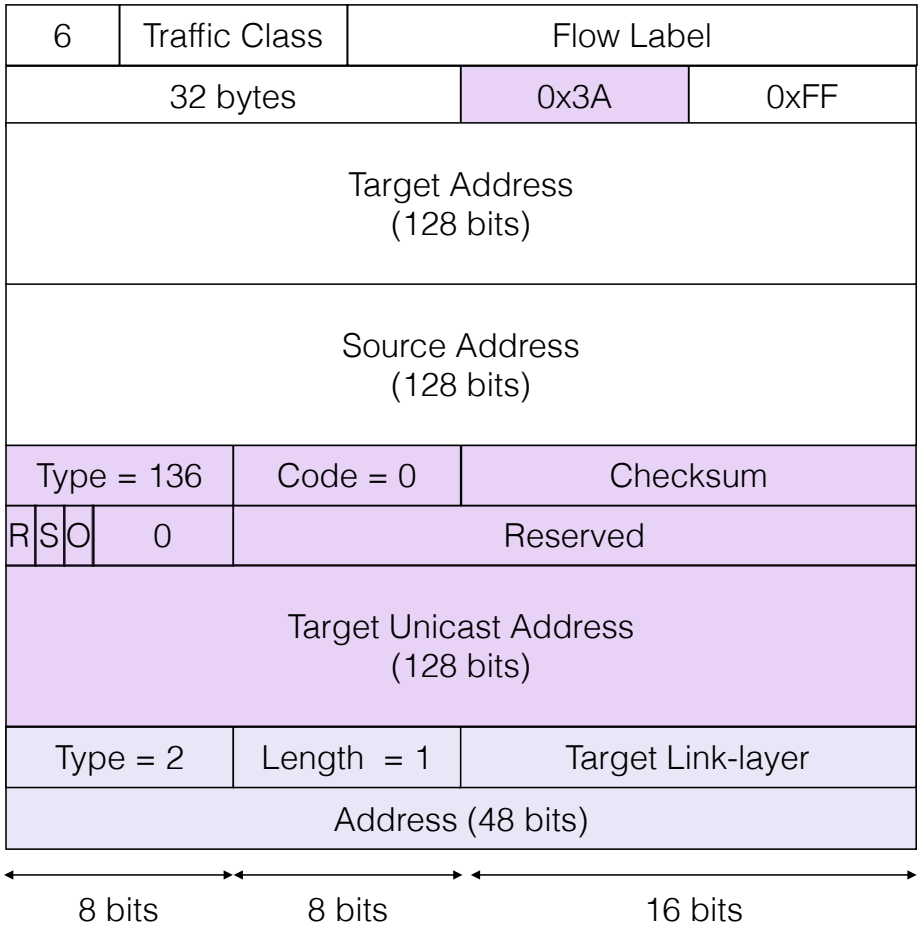
Type	Code	Nature
133	0	Router Solicitation
134	0	Router Advertisement
135	0	Neighbor Solicitation
136	0	Neighbor Advertisement
137	0	Redirection

Résolution des adresses IPv6-MAC

Neighbor Solicitation



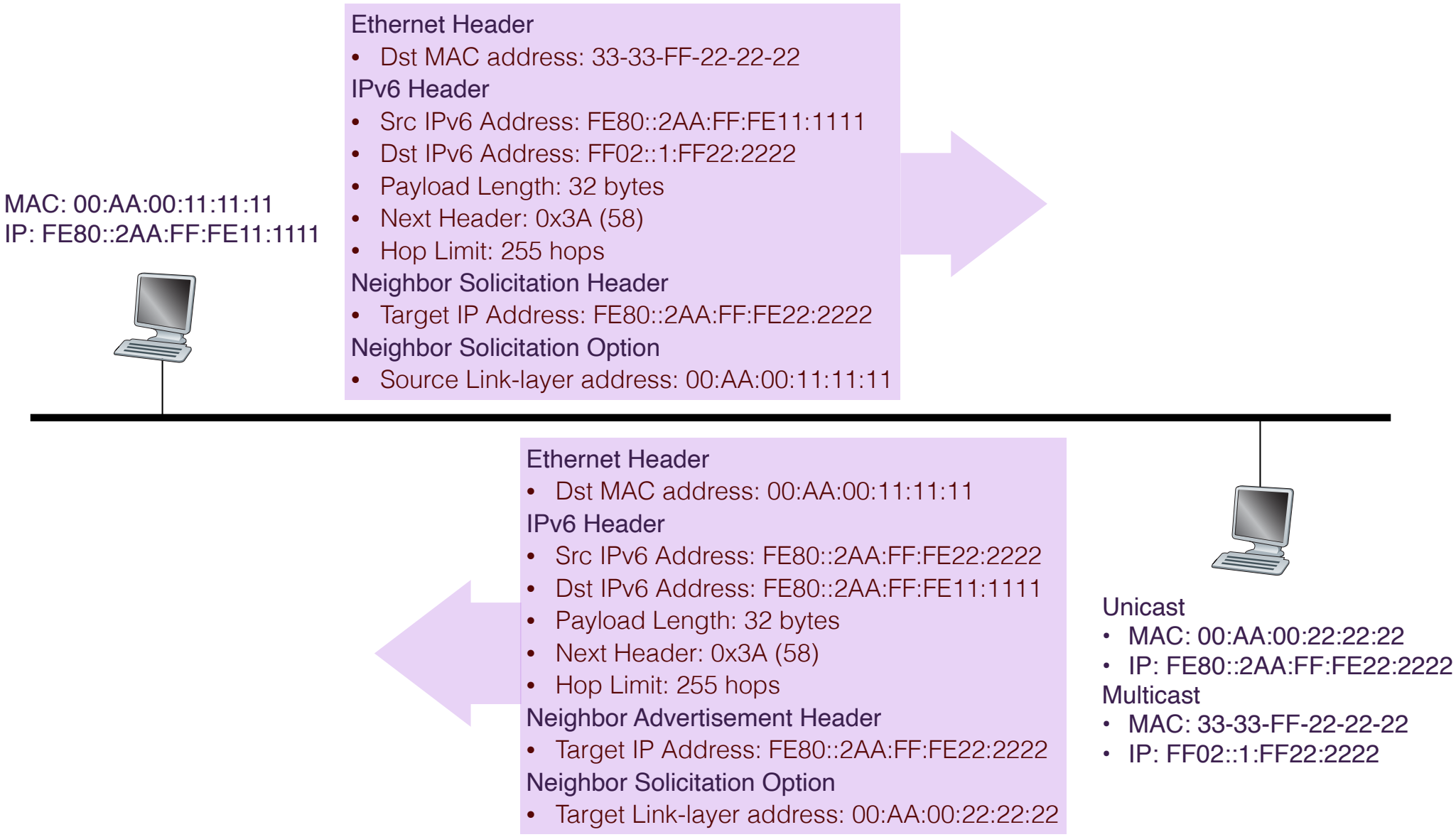
Neighbor Advertisement



Résolution des adresses IPv6 vers MAC

- Neighbor Solicitation (NS)
  - Pour découvrir l'address physique d'un voisin, la source :
    - envoie un NS contenant son adresse physique (Link-Layer Address option Type 1)
    - le NS est encapsulé dans un paquet IPv6 envoyé à l'adresse de nœud sollicitée déduite de l'adresse IP de la cible
    - le paquet IPv6 est encapsulé dans une trame envoyée à l'adresse MAC multicast correspondant à l'adresse de nœud sollicitée de la cible
- Neighbor Advertisement (NA)
  - Sur réception du message NS, la cible :
    - met à jour sa table de voisins avec la correspondance adresses IPv6-MAC de la source
    - envoie un NA en unicast contenant l'adresse physique de la cible (Link-Layer Address option Type 2)
  - Drapeaux RSO flags:
    - Drapeau Router – positionné à 1 si la cible est un routeur et à 0 sinon
    - Drapeau Solicited – positionné à 1 pour indiquer que le NA est retourné en réponse à un NS
    - Drapeau Override – positionné à 1 pour indiquer que l'adresse physique dans l'option Target Link-Layer Address doit écraser l'adresse physique si présente dans la table de voisins

Résolution des adresses IPv6-MAC



Conclusion

- Paquet IPv4
  - Taille max de l'entête : 60 octets
    - entête fixe : 20 octets
    - options IP : entre 0 et 40 octets
  - Fragmentation
    - ajuster la taille des paquets au champ données des trames
- Protocole ARP
  - Découvrir l'adresse MAC d'une machine voisine à partir de son adresse IP
  - Utilisation des tables ARP ou du broadcast Ethernet sinon
- Protocole ICMP
  - Tester la connectivité (ping et traceroute)
  - Diagnostiquer les erreurs de routage ou de livraison
- Cours prochain
  - DCHP, ARP et NAT