Adressage Privé / NAT

David Bromberg

Adresses publiques
≠ Adresses privées

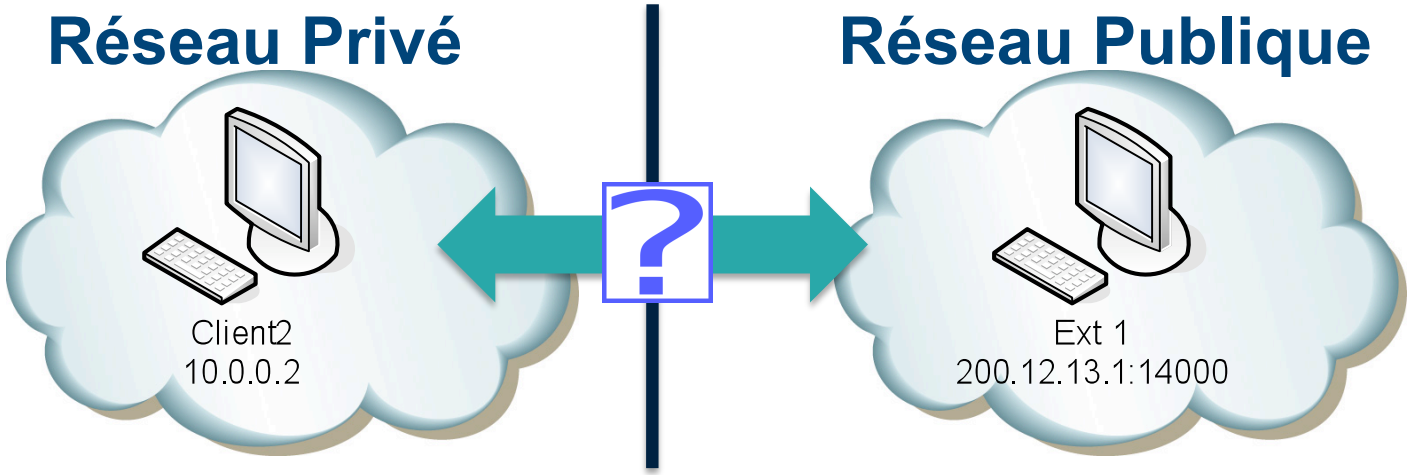
RFC 1918

- **Adresses privées**
  - Adresses qui ne seront jamais attribuées (adresses illégales)
  - Adresses non routables sur l'Internet
- **Trois plages d'adresses privées**
  - **Classe A :**
    - De 10.0.0.0 à 10.255.255.255
  - **Classe B :**
    - De 172.16.0.0 à 172.31.255.255
  - **Classe C :**
    - De 192.168.0.0 à 192.168.255.255

Adresses privées

RFC 1631

Résolution de la pénurie d' @IP ?



- **Pénurie d'@IP**
  - => Besoin de translation des adresses (NAT).
  - Principe décrit dans la RFC 1631.

NAT

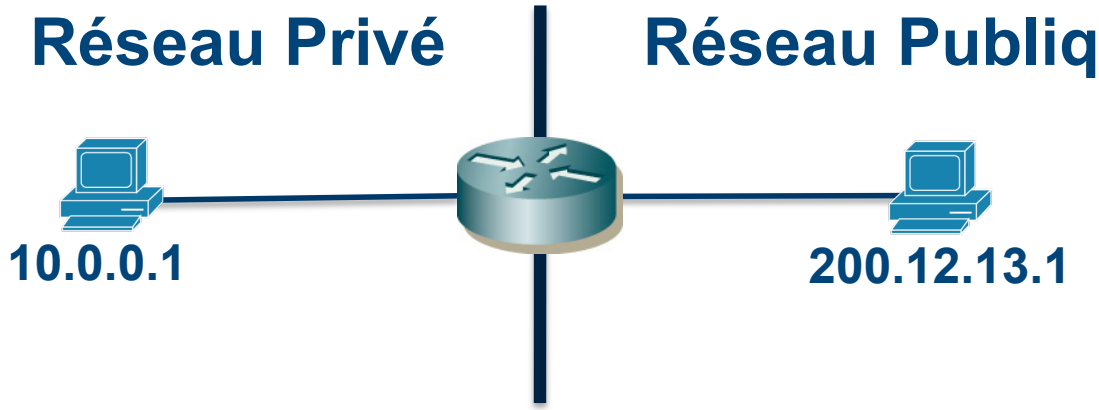
Présentation

RFC 1631

- Pourquoi le NAT
  - Pallier le problème de limitation du nombre d'adresses disponible par IPv4.
  - Permettre aux utilisateurs privés de ne payer qu'une seule connexion Internet, et d'avoir plusieurs postes.

NAT

Fonctionnement



- Table liant un couple (IP, Port) du réseau privé à un couple (IP,Port) du réseau Internet,
- Modification des entêtes IP/TCP des paquets entrants et sortants.

NAT

Problèmes

RFC 3489

- **Problèmes pour les protocoles ‘à contenu sale’,**
  - Échange au niveau applicatif des informations Réseau et ou Transport,
  - Un NAT Traditionnel ne modifie que les entêtes IP/TCP/UDP,
- **Différentes solutions NAT présentes.**

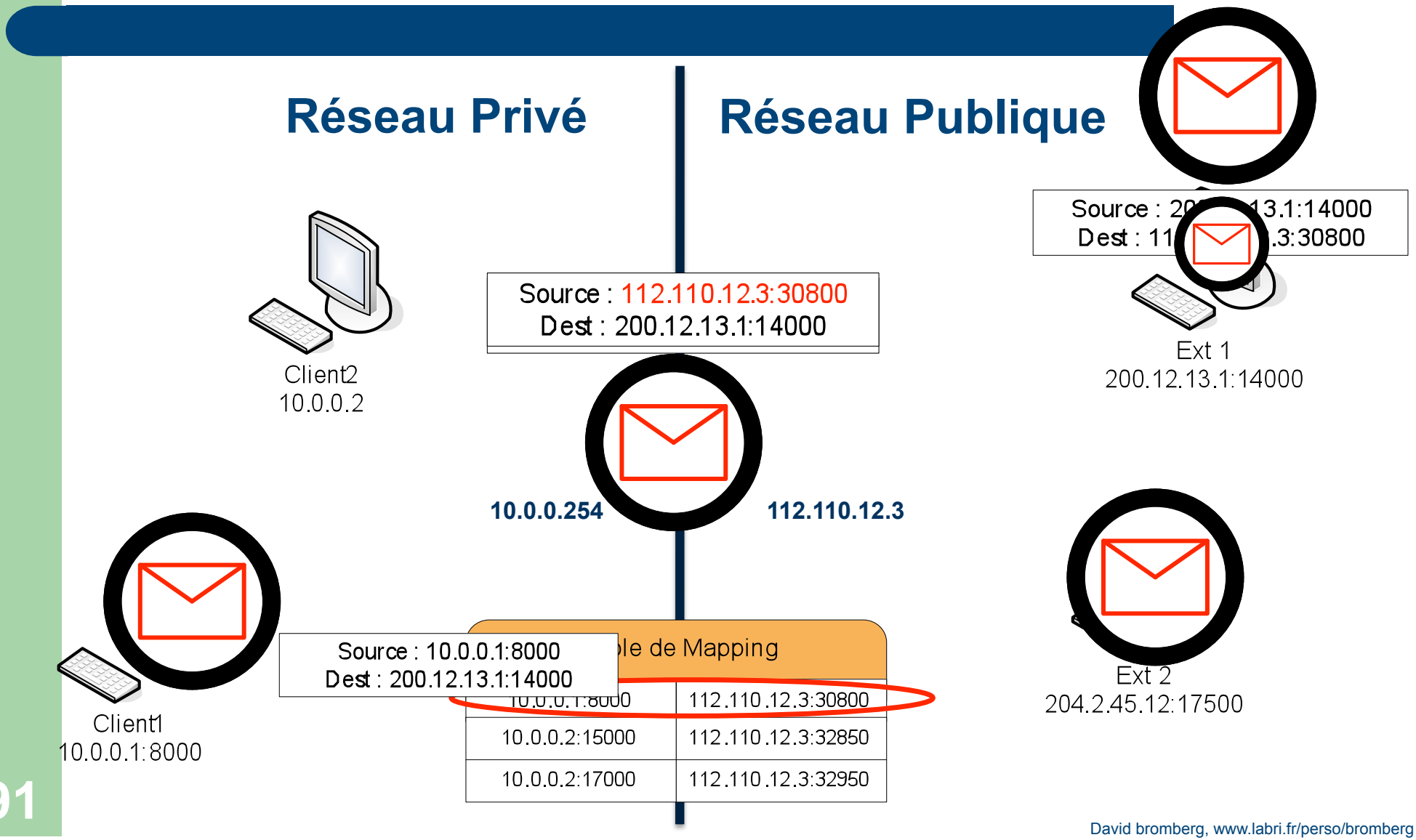
NAT – Full Cone

Définition

- Mapping unique entre une IP:Port privé et une IP:Port public,
  - Une seule entrée par couple (IP,Port) privé dans la table de mapping,
- N'importe quelles machines extérieures connaissant ce mapping peut communiquer avec le client,
- Problèmes de sécurité.

NAT – Full Cone

Fonctionnement



NAT – Restricted Cone
Définition

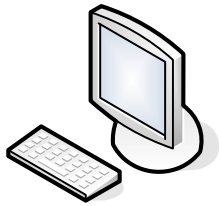
- Le mapping entre (IP, Port) privé et (IP, Port) public n'existe qu'à partir du moment où le client privé établi la communication,
- Un extérieur ne peut pas initier la communication contrairement à ***Full Cone***,
- Même fonctionnement que ***Full Cone*** pour les utilisateurs autorisés.

NAT – Restricted Cone

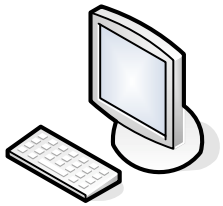
Fonctionnement

Réseau Privé

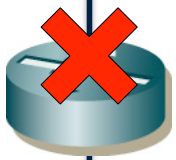
Réseau Publique



Client2
10.0.0.2



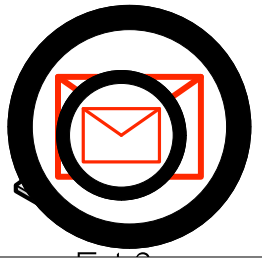
Ext 1
200.12.13.1:14000



10.0.0.254

112.110.12.3

Source : 10.0.0.1:8000
Dest : 200.12.13.1:14000



Source : 204.2.45.12:17500
Dest : 112.110.12.3:30800

Table de Mapping

10.0.0.1:8000	112.110.12.3:30800	200.12.13.1
10.0.0.2:15000	112.110.12.3:32850	IP ext autorisés
10.0.0.2:17000	112.110.12.3:32950	IP ext autorisés

NAT – Port Restricted Cone
Définition

- Même fonctionnement que le restricted cone,
- Cependant seuls les paquets venant du couple (IP,PORT) distants connus sont acceptés par le NAT.

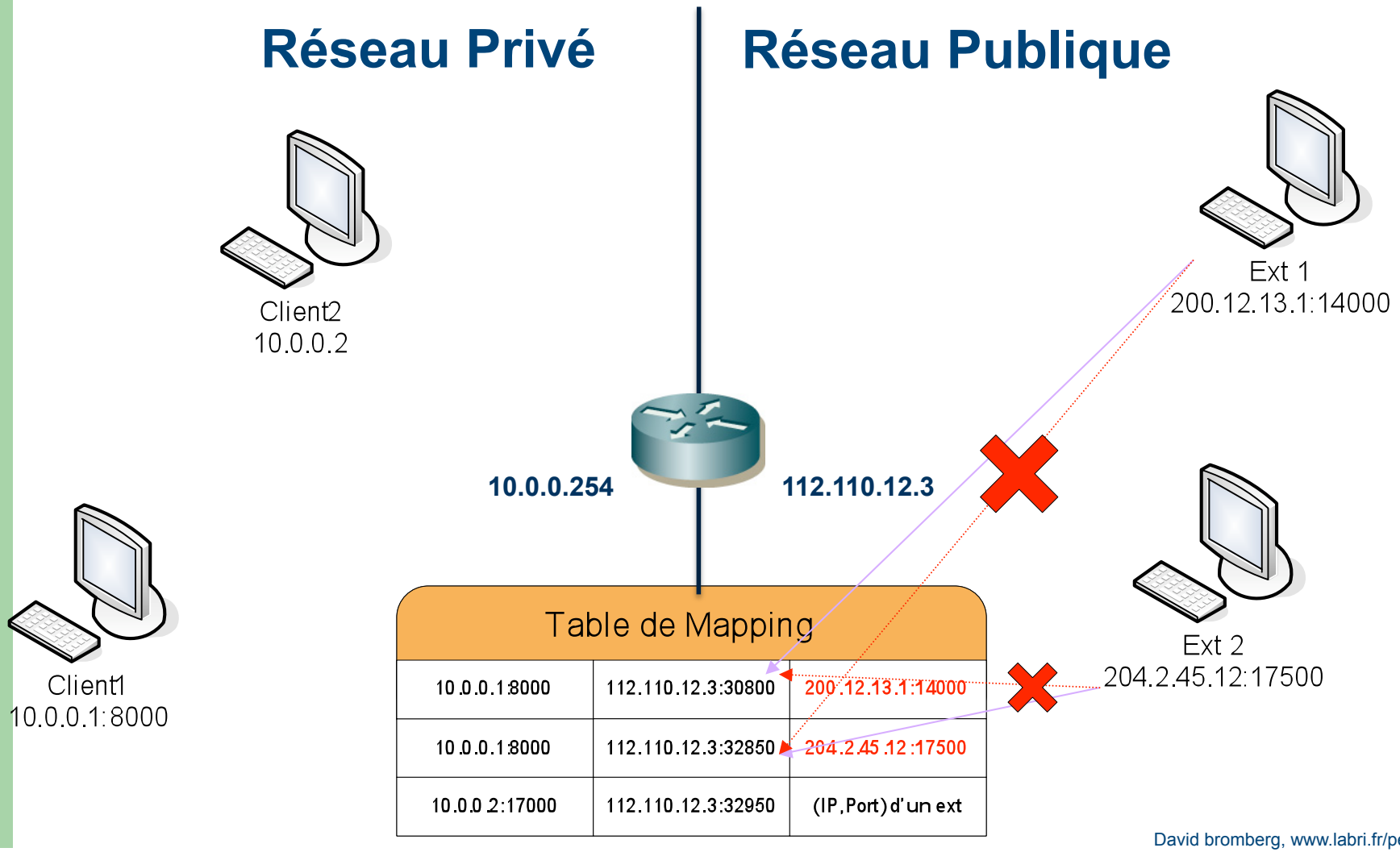
NAT – Symétrique

Définition

- Le *mapping* dépend :
  - A la fois du couple(i@IP,iPort) privé du client et
  - A la fois du couple (e@IP,ePort) de l'extérieur.
- Pour le même couple (i@IP,iPort),
  - si la destination (e@IP,ePort) est différente,
  - ⇔ Un autre *mapping* est utilisé.
- Ce mapping ne peut être initié que par le client.

NAT – Symétrique

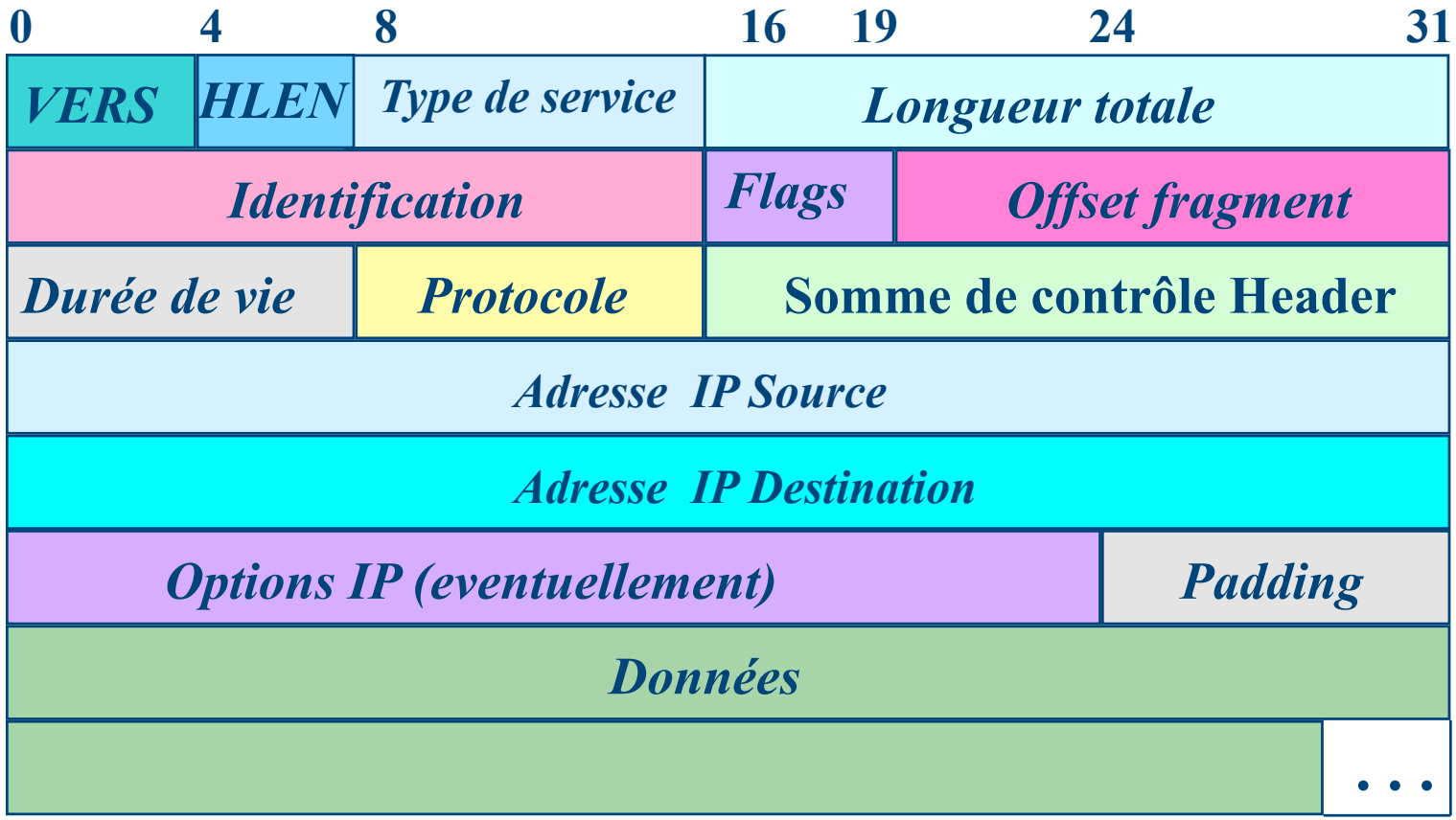
Fonctionnement



Datagramme IP

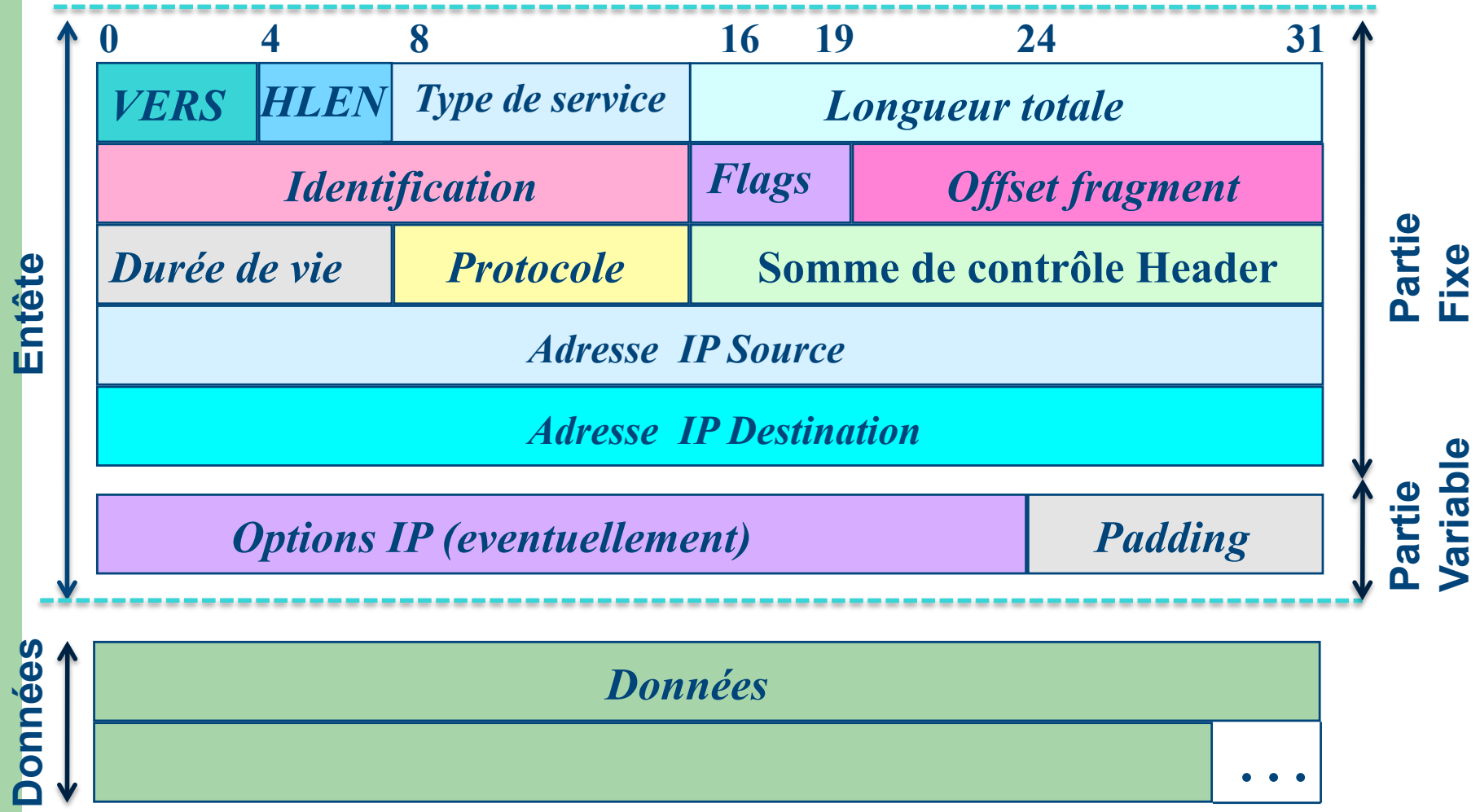
Datagramme IP

Aperçu

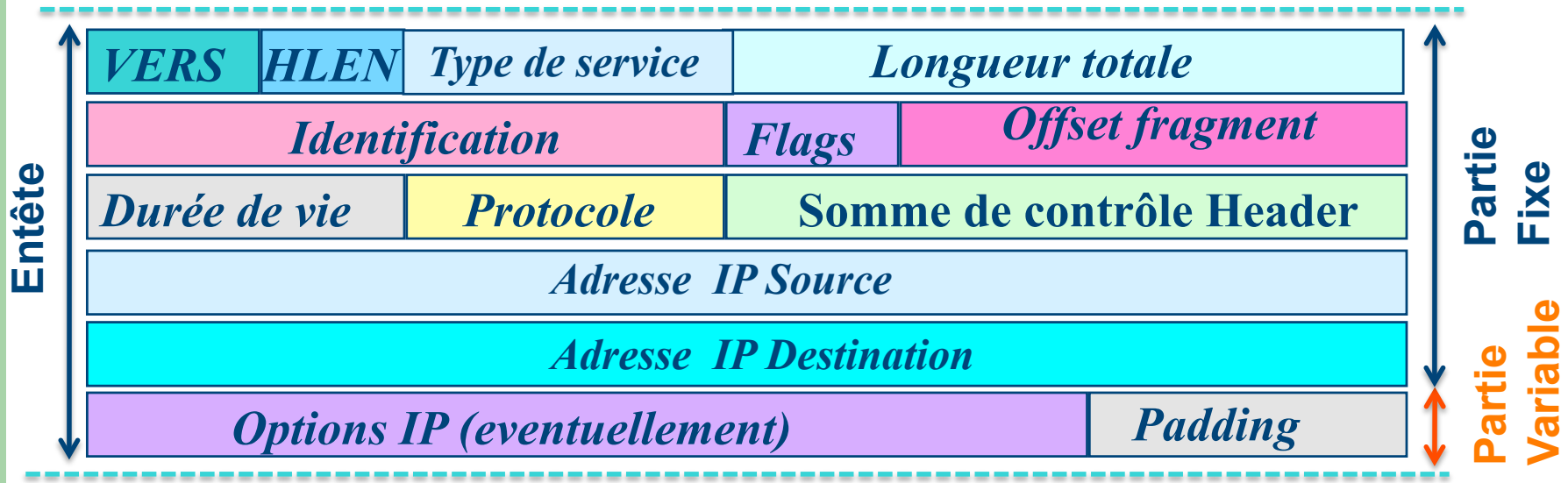


Datagramme IP

Décomposition

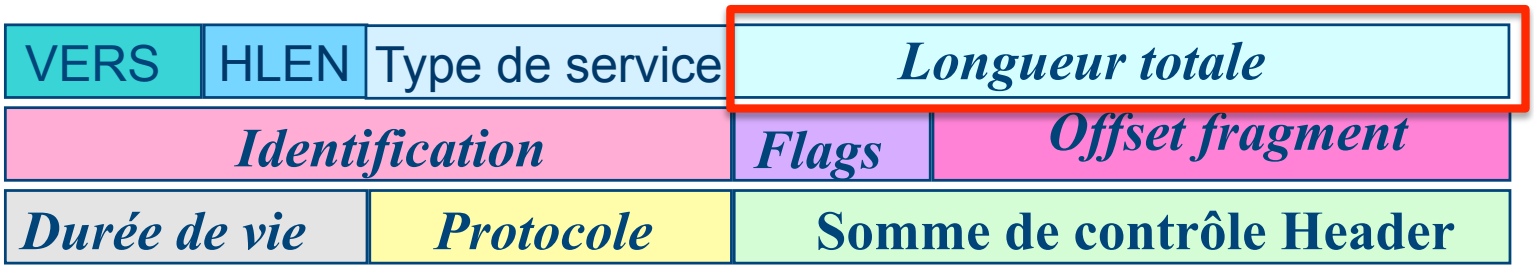


Les champs du datagramme IP
Vers, Hlen,



- **VERS :**
  - Numéro de version de protocole IP, actuellement version 4,
- **HLEN :**
  - Longueur de l'en tête non constante
    - 4bits qui donnent la longueur de l'en-tête en mots de 4 octets (32 bits).
    - Taille minimum : 5 mots => 20 octets (sans les options)
    - Taille maximum : 15 mots => 60 octets
    - Reste 40 octets pour les options (souvent insuffisant)

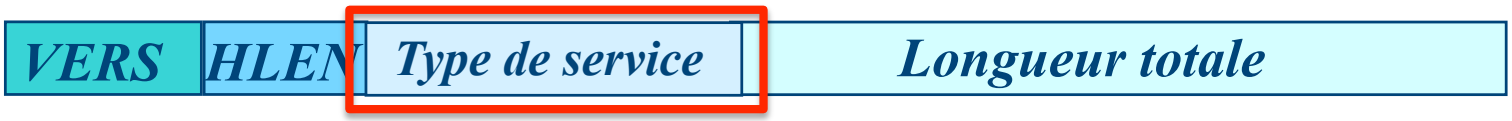
Les champs du datagramme IP
Longueur totale



- ***Longueur totale :***
  - Donne la taille du datagramme, en-tête plus données.
  - S'il y fragmentation (voir plus loin) il s'agit également de la taille du fragment (chaque datagramme est indépendant des autres).
  - La taille des données est donc à calculer par soustraction de la taille de l'en-tête.
  - **Longueur maximale : 65 535 octets**
    - ⇔ **Insuffisant pour les réseaux gigabits du futur**

Les champs du datagramme IP

Type de service :



- ***Type de service :***
  - 8 bits (4 utiles) qui indiquent au routeur l'attitude à avoir vis à vis de ce datagramme.
  - Suivant les valeurs de ce champ, le routeur peut privilégier un datagramme par rapport à un autre.

    - PRECEDENCE (3 bits) :
      - Définit la priorité du datagramme;
      - Valeurs de 0 à 7
      - En général ignoré par les machines et passerelles.
    - Bits D, T, R :
      - Indiquent le type d'acheminement désiré du datagramme, permettant à une passerelle de choisir entre plusieurs routes (si elles existent) :
        - D signifie délai court,
        - T signifie débit élevé
        - R signifie grande fiabilité.

        ⇔ En théorie aide les routeurs à choisir entre une liaison plutôt qu'une autre

Fragmentations
LE MTU

?

- **MTU (*Maximum Transfert Unit*)**
  - Une unité maximale de transfert
  - Définit la taille maximale d'un datagramme véhiculé sur le réseau physique correspondant.
- **Lorsque le datagramme est routé vers un réseau physique dont le MTU est plus petit que le MTU courant :**
  - La passerelle fragmente le datagramme en un certain nombre de fragments.

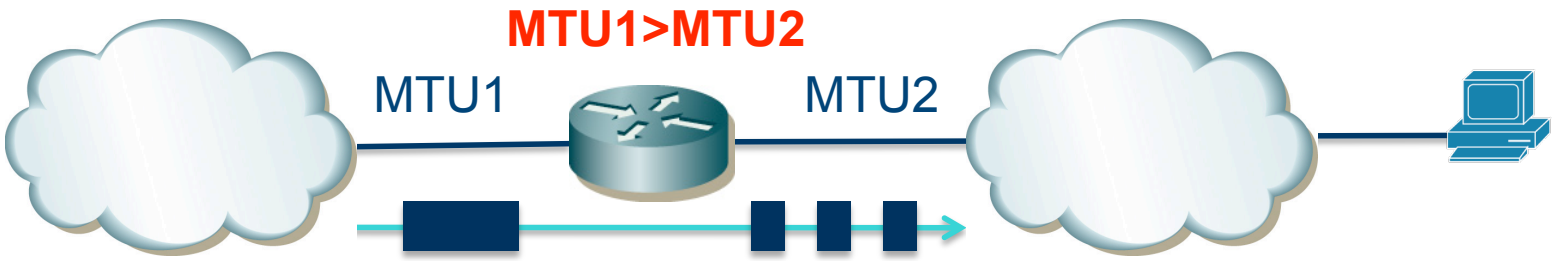
Fragmentations
IDENTIFICATION, FLAGS …

Identification	*Flags*	*Offset fragment*

- **Ces champs sont prévus pour :**
  - **Contrôler la fragmentation des datagrammes**
- **Fragmentation des données :**
  - **Les datagrammes peuvent avoir à traverser des réseaux avec des MTU plus petits que celui du premier support physique employé.**

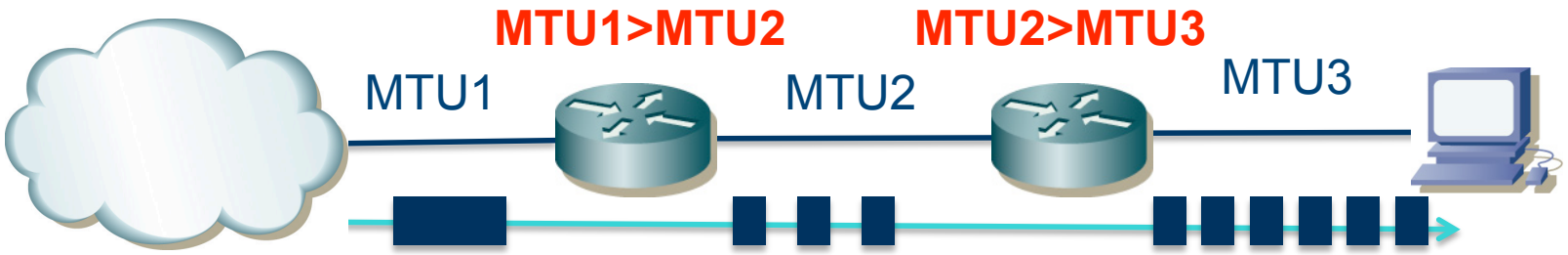
Fragmentations

Fonctionnement (1)



- Lorsque le datagramme est routé vers un réseau physique dont le MTU est supérieur au MTU courant, le routeur route les fragments tels quels.

Fragmentations
Fonctionnement (2)



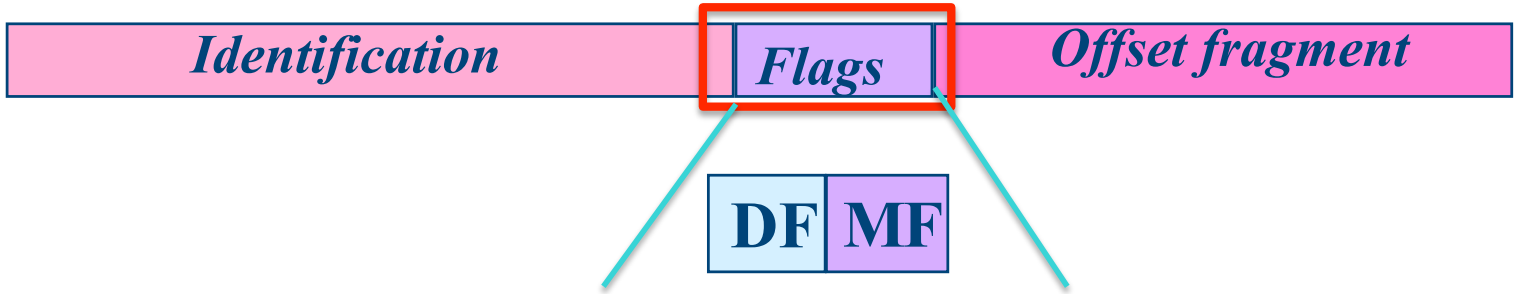
- Le destinataire final reconstitue le datagramme initial à partir de l'ensemble des fragments reçus;
  - La taille de ces fragments correspond au plus petit MTU emprunté sur le réseau.
  - Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu :
  - La probabilité de perte d'un datagramme augmente avec la fragmentation.

Fragmentations
Exemple

Le MTU est de 1500 pour une trame Ethernet, elle peut être de 256 avec SLIP (``Serial Line IP'') sur liaison série (RS232...).

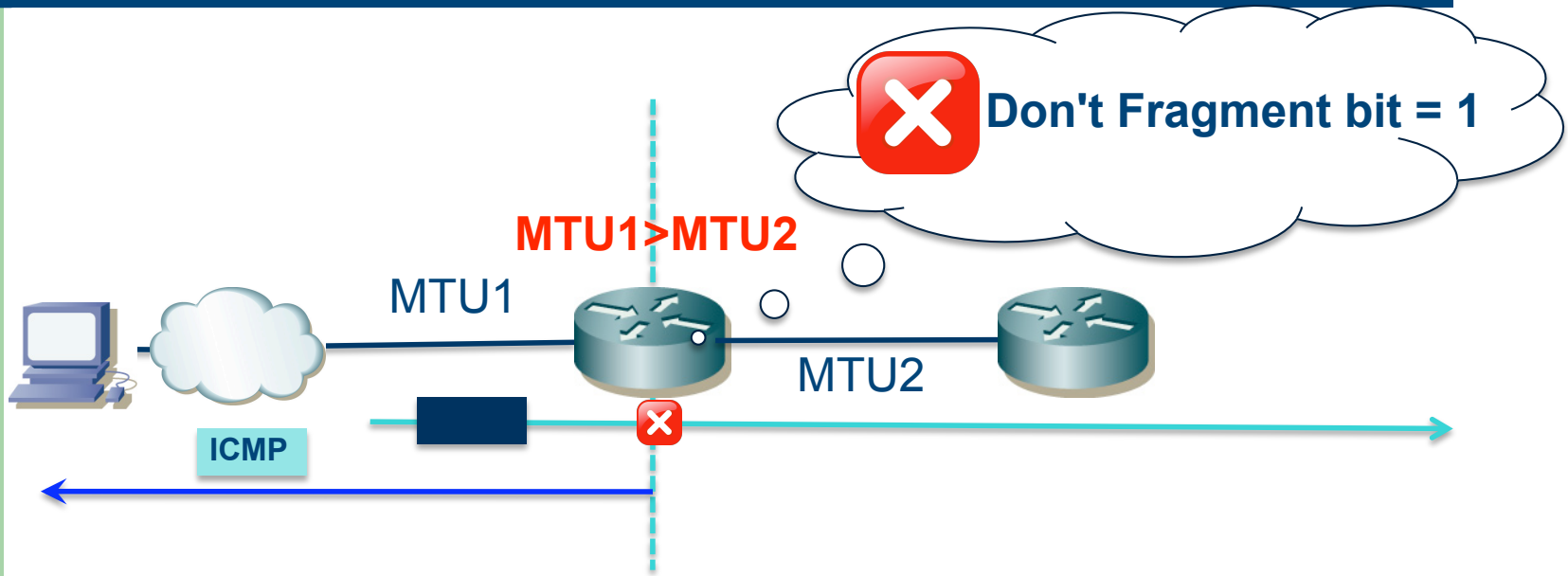
- Dans ces conditions, si la couche IP doit transmettre un bloc de données de taille supérieure au MTU à employer, il y a fragmentation !
- Un bloc de 1481 octets sur Ethernet sera décomposé en un datagramme de 1480
  - (1480 + 20 = 1500) et un datagramme de 1 octet !

Fragmentations
L'exception (1)



- Il existe une exception à cette opération
  - Bit **Don't Fragment bit** (DF) du champ FLAGS de l'en-tête IP.
  - La présence à 1 de ce bit interdit la fragmentation dudit datagramme par la couche IP qui en aurait besoin.
- Bit More Fragment (MF) activé dans tous les fragments d'un datagramme excepté le dernier.

Fragmentations
L'exception (2)



- Situation de blocage,
  - Peut conduire à la perte du fragment
  - ⇔ la couche émettrice est tenue au courant par un message ICMP
    - *Fragmentation needed but don't fragment bit set* et bien sûr le datagramme n'est pas transmis plus loin.

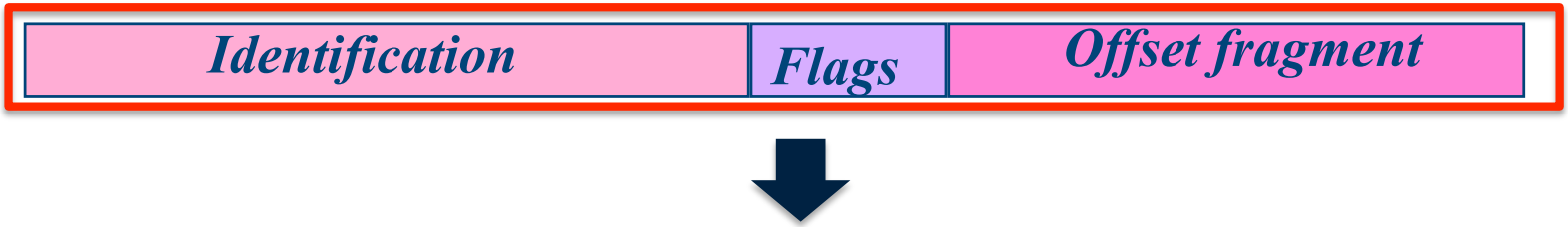
Fragmentations

Que devient un fragment ?

- Les fragments deviennent des datagrammes à part entière.
- Rien ne s'oppose à ce qu'un fragment soit à nouveau fragmenté.
- Absolument transparente pour les couches de transport qui utilisent IP.

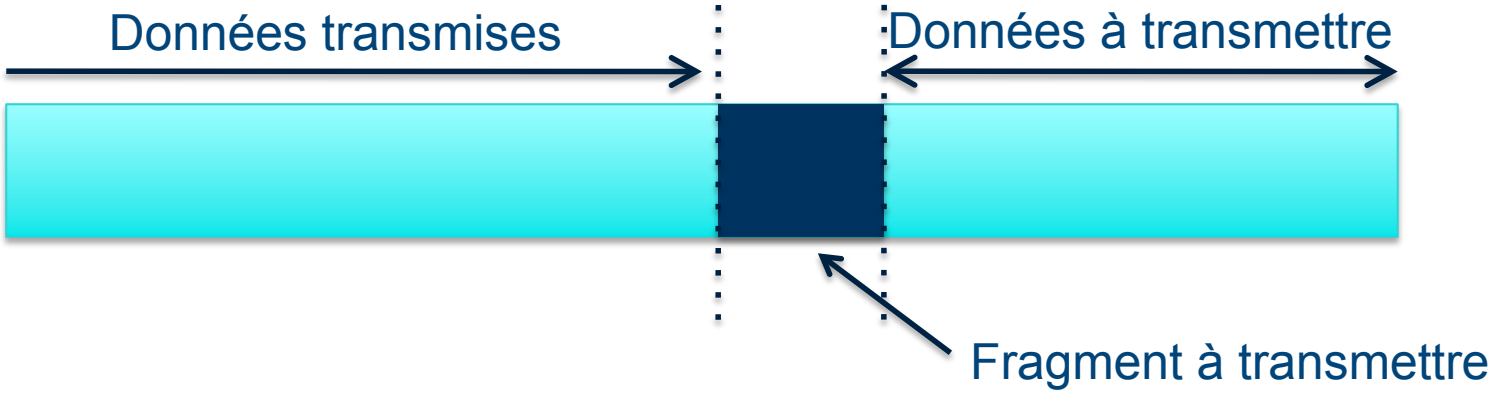
Fragmentation

Fonctionnement interne



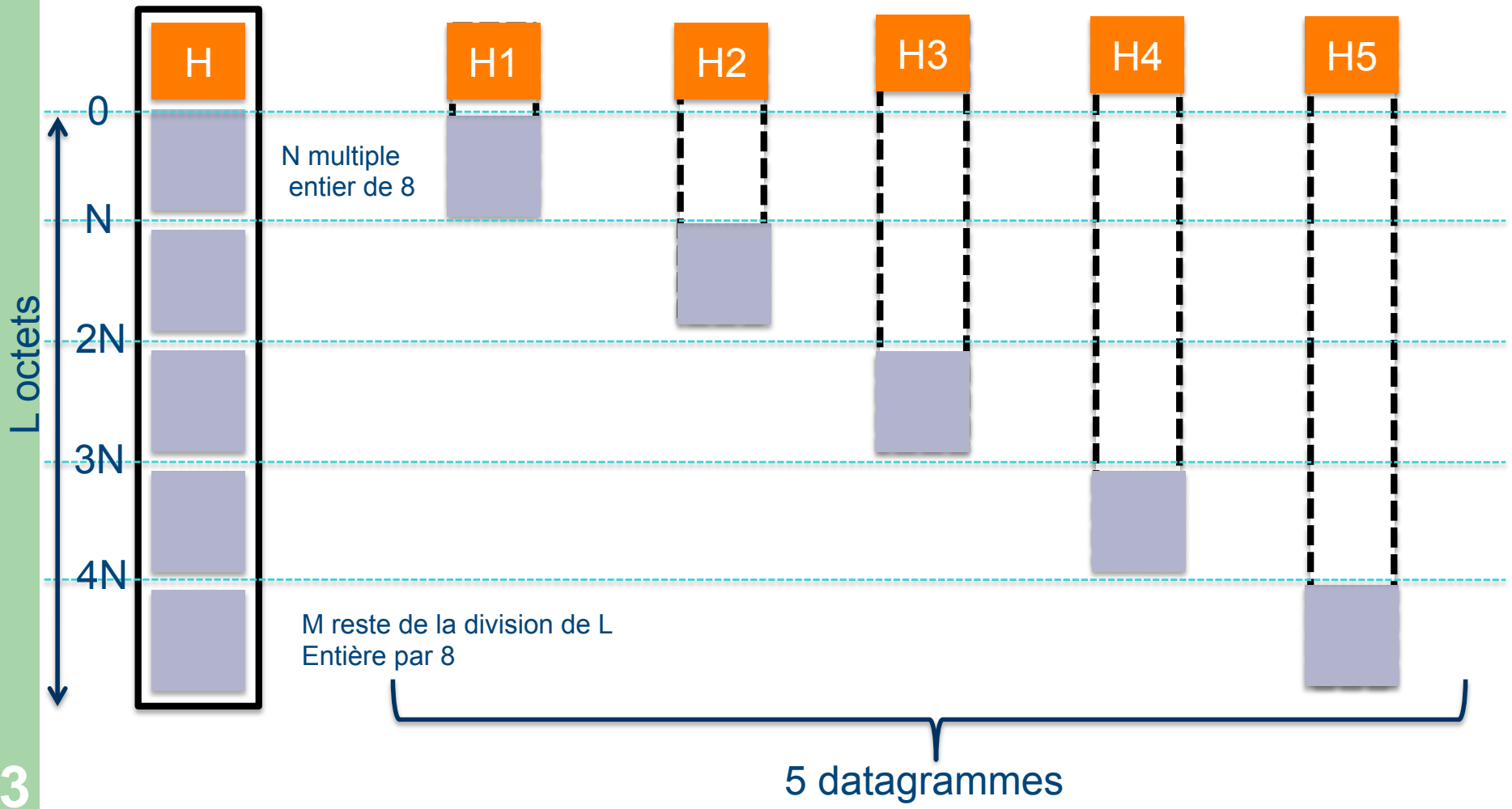
- Chaque fragment est identifié de manière unique, relativement au datagramme initial.
- Cette valeur est inscrite dans le champ *IDENTIFICATION.*
- S'il y a encore des fragments, un des bits du champ *FLAGS* est positionné à 1 pour indiquer ‘More fragment***!*** ‘
- *FRAGMENT OFFSET* contient l'offset du fragment, relativement au datagramme initial.

Fragmentation
Offset (1)

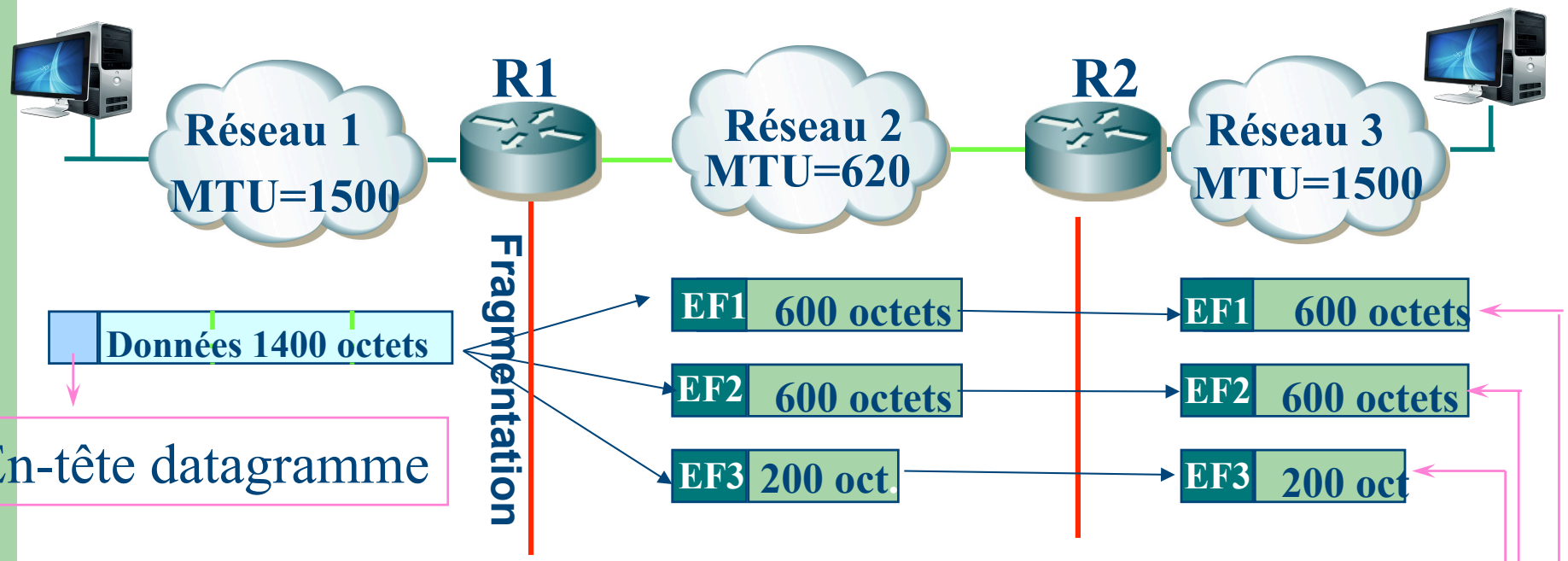


- Les données doivent faire un multiple de 8 octets, sauf pour le dernier fragment.
- Le champ TOTAL LENGTH change.
- Chaque fragment est un datagramme indépendant, susceptible d'être à son tour fragmenté.
- Pour le dernier fragment :
  - FLAGS est remis à zéro.
  - Les données ont une taille quelconque.

Fragmentation
Offset (2)



Fragmentation
Offset(3)



- EF1 et EF2 ont le bit More (M) positionné.
- Le déplacement (depl) est relatif au datagramme initial.

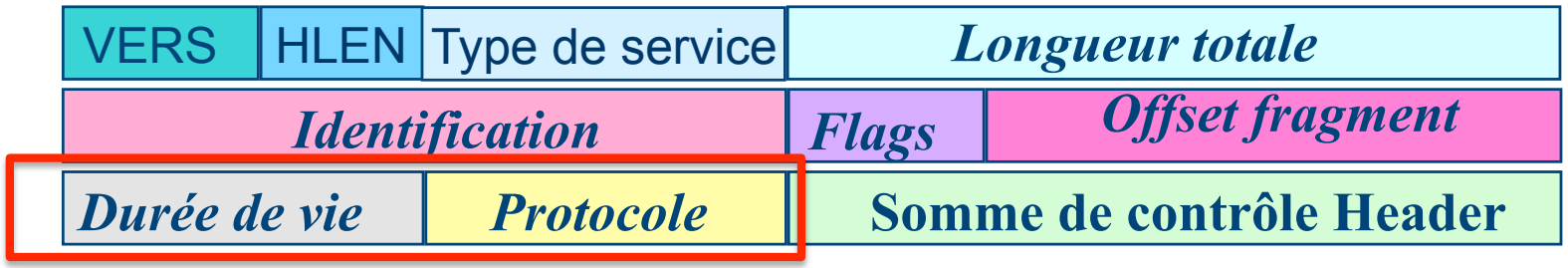
En-tête fragments: M=0; depl=1200

En-tête fragments: M=1; depl=600

En-tête fragments: M=1; depl=00

Les champs du datagramme IP

Durée de vie, Protocole



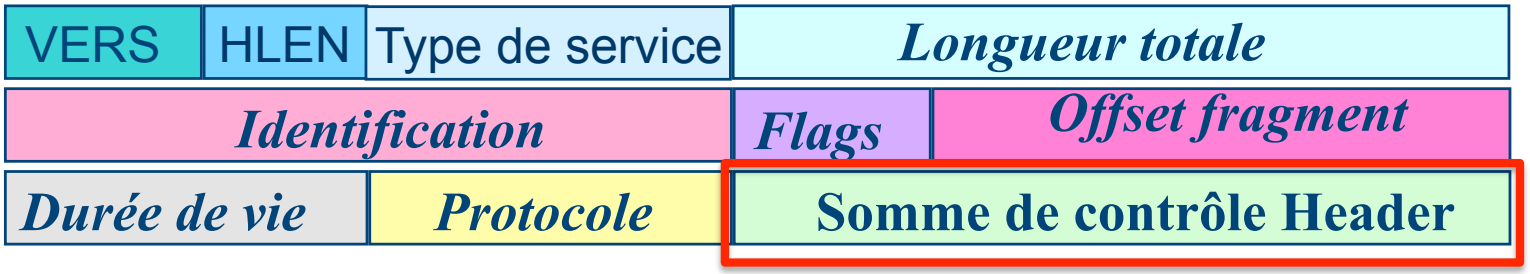
- ***Durée de vie***
  - Indique en secondes, la durée maximale de transit du.
  - La machine qui émet le datagramme définit sa durée de vie.
  - Les routeurs qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans le routeur;
  - Lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.
- ***Protocole***

  Ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :

  - 6 : TCP,
  - 17 : UDP,
  - 1 : ICMP.

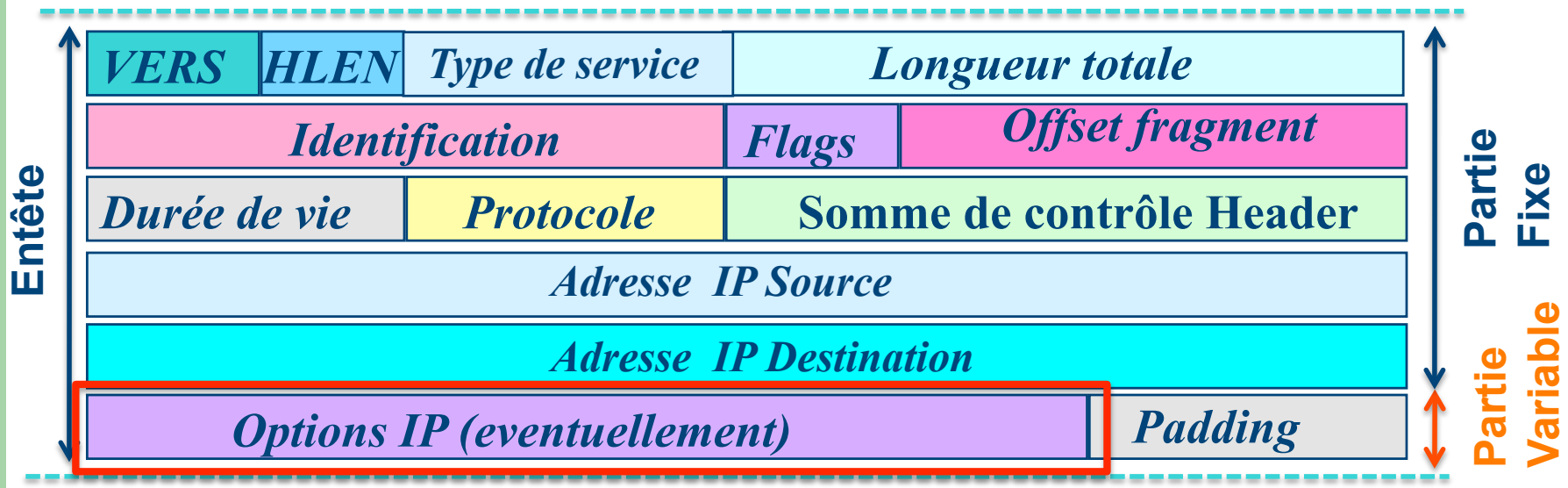
  RFC 1700

Les champs du datagramme IP
Somme de contrôle de l'en-tête



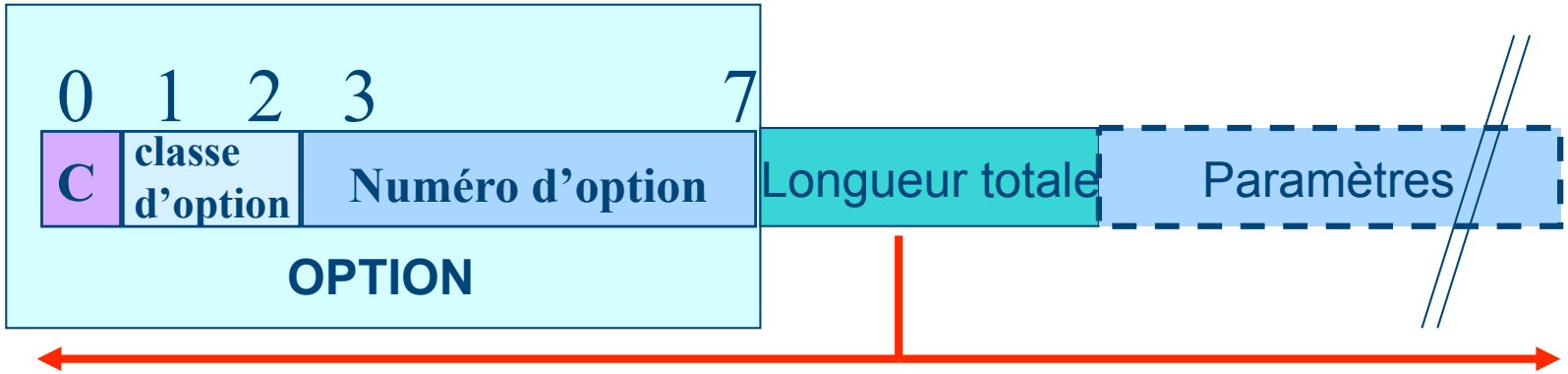
- ***Somme de contrôle de l'en-tête***
  - Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme.

Les options



- Le champ OPTIONS est facultatif et de longueur variable.
  - Les options concernent essentiellement des fonctionnalités de mise au point.
  - Débute par un code d'identification de 1 octet

Les options
Structure



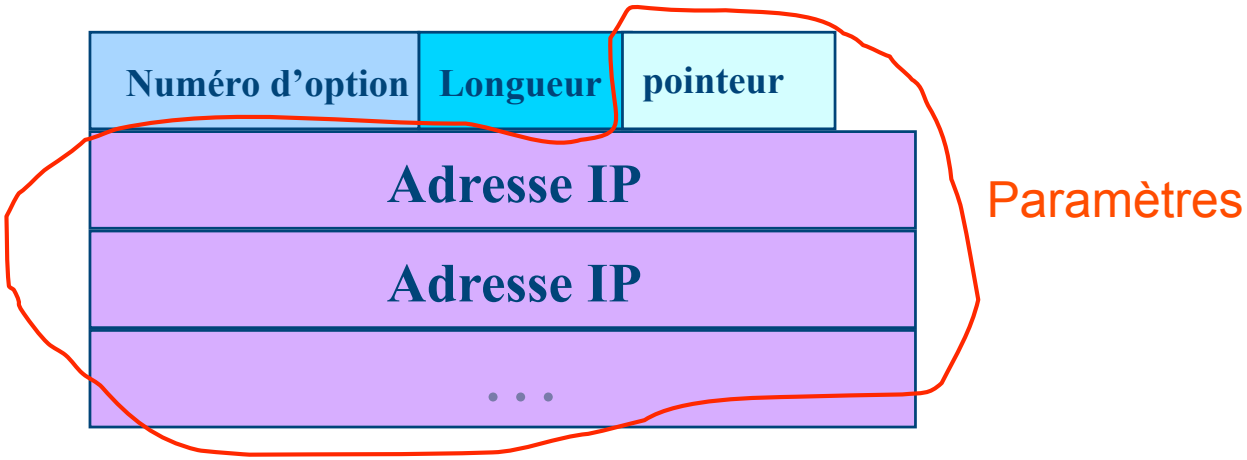
- Le champ option doit être un multiple de 4 octets
- C indique que l'option doit être recopiée dans tous les fragments (c=1) ou bien uniquement dans le premier fragment (c=0).

- Les bits classe d'option
  - 00 : contrôle
  - 01 : réservé pour un usage ultérieur
  - 10 : option pour le déboguage et les mesures
  - 11 : réservé pour un usage ultérieur

- Un numéro d'option indiquent le type de l'option et une option particulière

- Si une option nécessite des arguments, on ajoute un champ longueur codé sur un octet donnant la longueur totale de l'option, suivi des paramètres.

Option
Record Route (RR) (1)



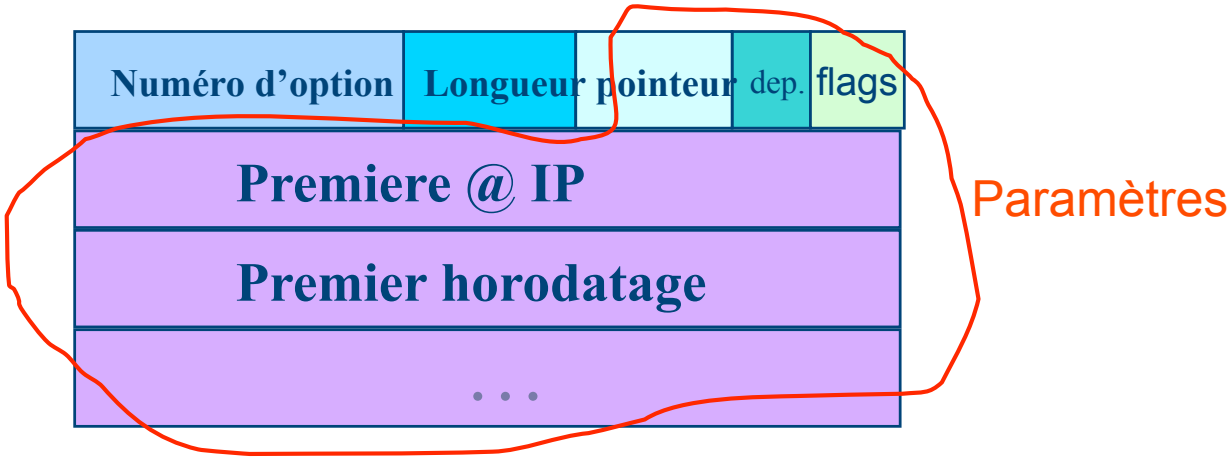
- Enregistrement de route **(classe = 0, option = 7)**
  - Permet à la source de créer une liste d'adresse IP vide et de demander à chaque routeur d'ajouter son adresse dans la liste.
  - Permet de détecter les bogues des algorithmes de routages.

Option
Record Route (RR) (2)

Peut-on vraiment enregistrer l'@IP de tous les routeurs traversés?

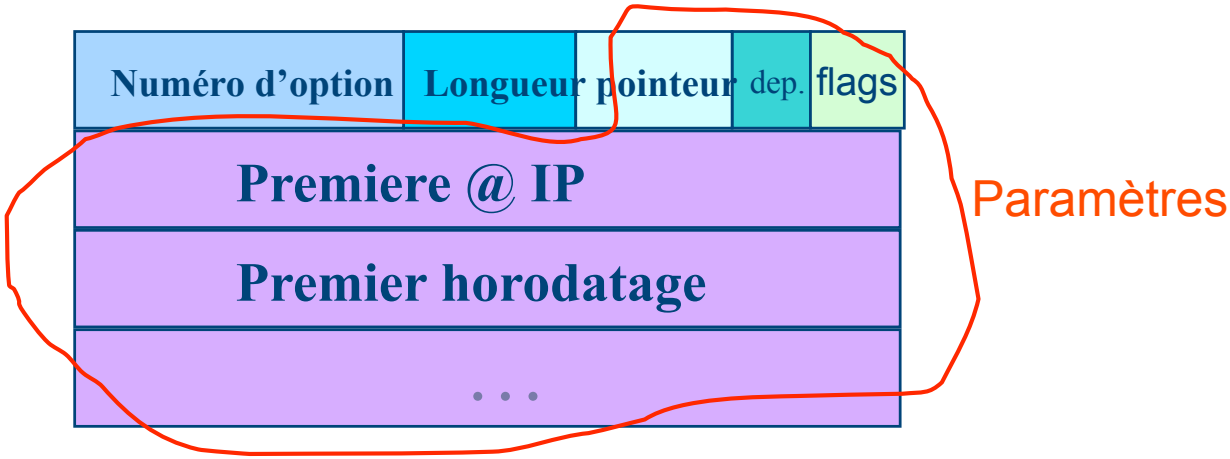
- A l'origine, avec ARPANET le routage d'un datagramme ne pouvait pas inclure plus de neuf routeurs !!
- Ne pas oublier que la taille maximale du champs options ne peut pas dépasser 40 octets !!

Options
Horodatage (1)



- Horodatage **(classe = 2, option = 4)**
  - Même fonctionnement que RR
  - Permet d'obtenir les temps de passage (timestamp) des datagrammes dans les routeurs.
  - Exprimé en heure et date universelle.

Options
Horodatage (2)



- Une liste de couples (adresse IP - horodatage) est réservée par l'émetteur; les passerelles ont à charge de remplir un champ lors du passage du datagramme.

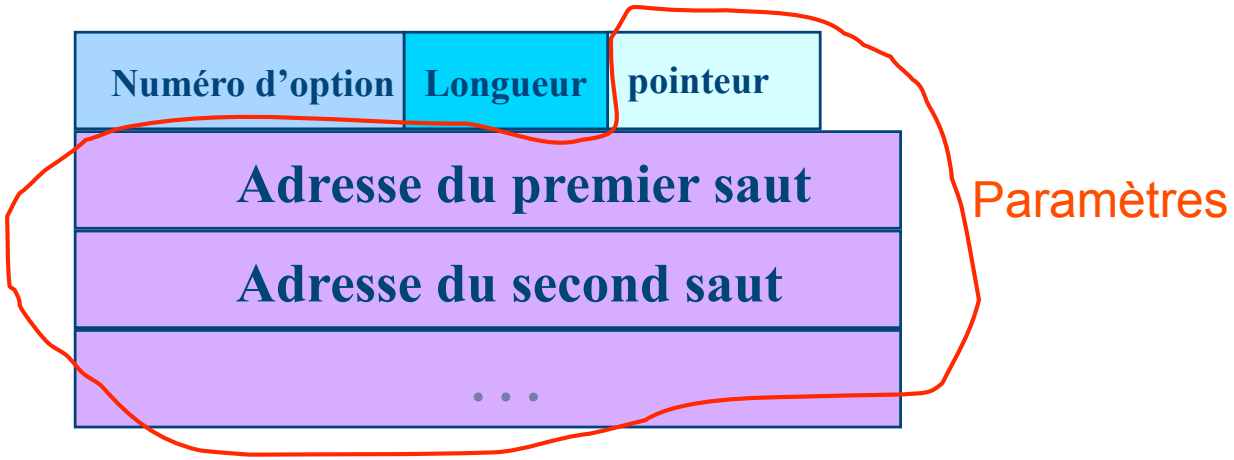
Options
Horodatage (3)

- Le champ dépassement de capacité (dep.) comptabilise les routeurs qui n'ont pu fournir les informations requises (liste initiale était trop petite).

- **Plusieurs mode de fonctionnement** :
  1. FLAGS = 0
     - Les routeurs doivent renseigner uniquement l'horodatage
  2. FLAGS = 1
     - L'horodatage et l'adresse IP
  3. FLAGS=3)
     - Si les adresses IP sont prédéfinies par l'émetteur, les passerelles n'indiquent l'horodatage que si l'adresse IP pointée par le champ *pointeur* est identique à leur adresse IP.

- Les horodatages, bien qu'exprimés en temps universel, ne constituent qu'une estimation sur le temps de passage car les horloges des machines situées sur les réseaux ne sont pas synchronisées.

Option
Strict source route (SSR)



- Routage strict prédéfini par l'émetteur **(classe = 0, option = 9)**
  - Prédéfinit le routage qui doit être utilisé dans l'interconnexion en indiquant la suite des adresses IP des routeurs.
  - Le chemin spécifié ne tolère aucun autre intermédiaire; une erreur est retournée à l'émetteur si un routeur ne peut appliquer le routage spécifié.