

Réseaux informatiques RXI

Chapitre 5 Les réseaux IP 2^{ème} partie



Objectifs d'apprentissage

- Savoir expliquer la structure d'Internet, notamment l'interconnexion des réseaux.
- Savoir calculer des plages d'adresses pour un masque de sous-réseaux
- Savoir distinguer des plages d'adresses privées
- Savoir expliquer le fonctionnement de NAT et NAPT
- Savoir expliquer les mécanismes du protocole IP

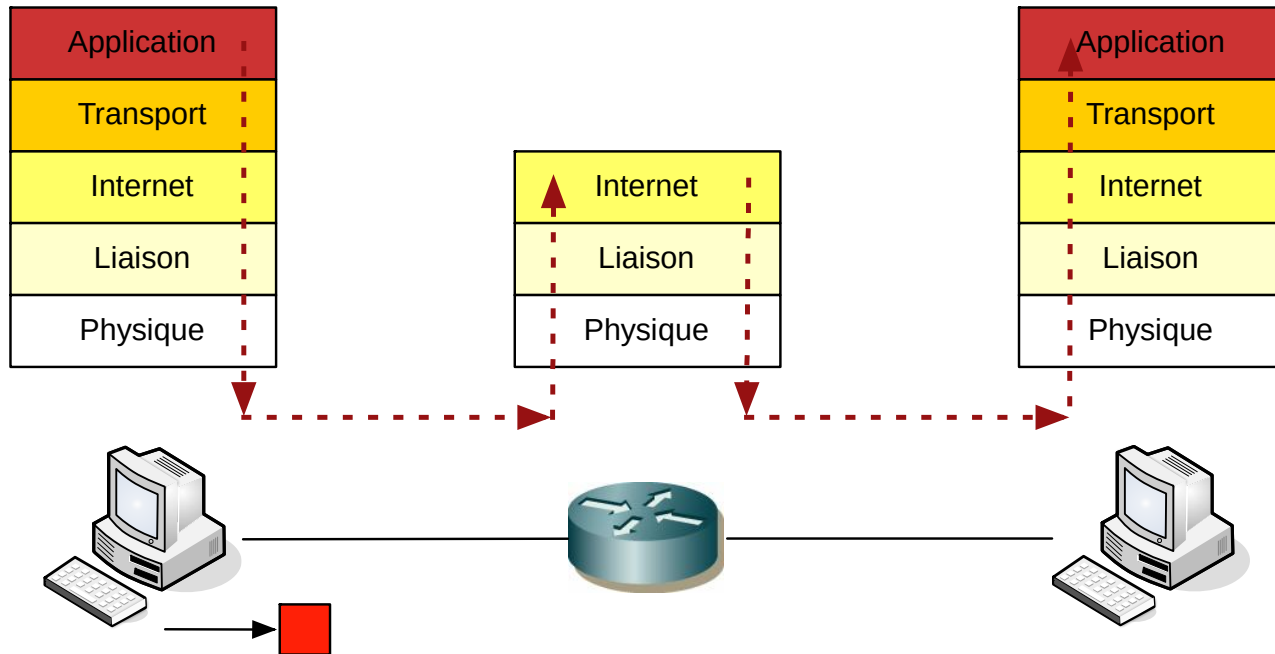


Service offert par IP

- **Transmission sans connexion**
 - Aucun établissement de connexion avant l'envoi des données
 - Un paquet (appelé « datagramme IP ») contient toutes les informations nécessaires à son traitement
- **Service non fiable « Best Effort » (Au mieux)**
 - IP essaie au mieux de transmettre les paquets, mais ne garantit rien
 - Les paquets peuvent être perdus, arriver en désordre, arriver en retard
- **Fragmentation et réassemblage**
 - Une source de paquets ne connaît pas le chemin emprunté, ni les technologies sous-jacentes. Elle ne peut pas anticiper la taille de paquet maximum possible
 - Les routeurs intermédiaires peuvent fragmenter un datagramme en plusieurs fragments plus petits



Modèle de service d'IP

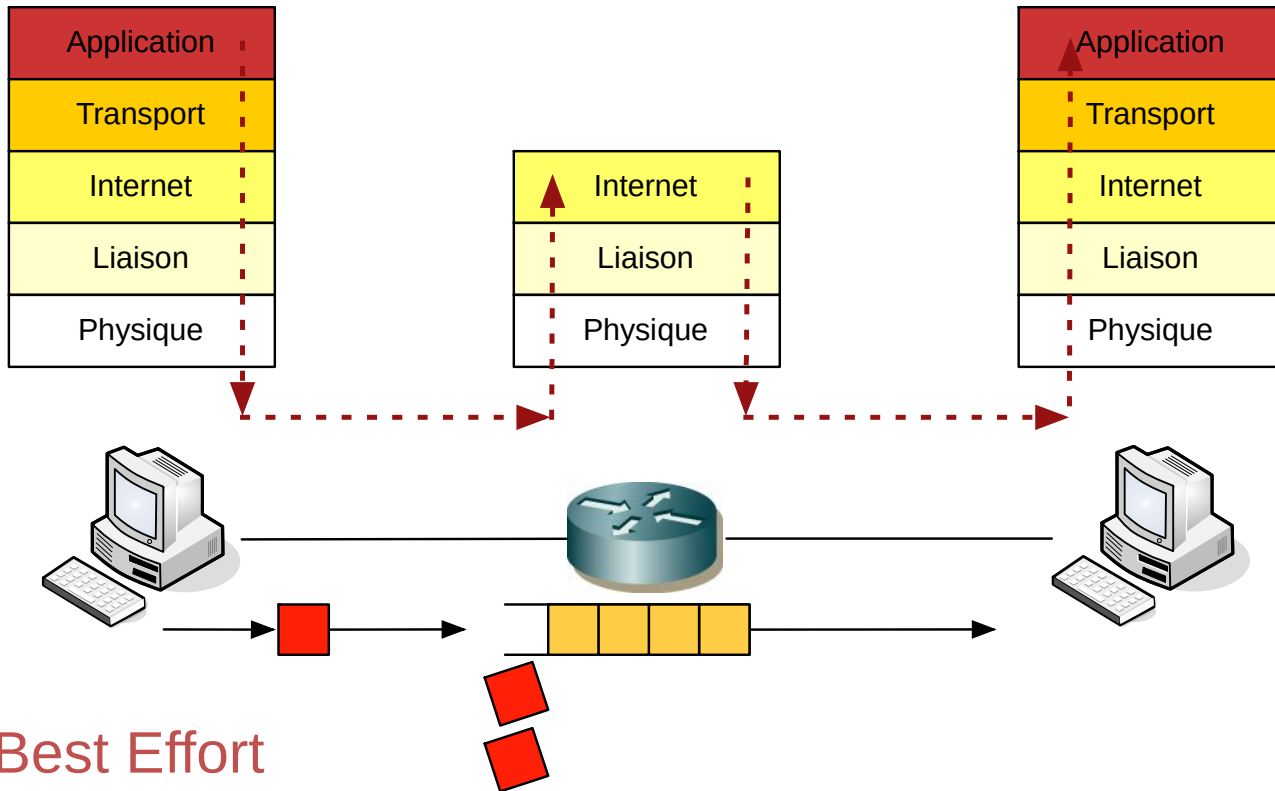


Sans connexion

- Une source peut envoyer des données à tout moment, sans connexion préalable



Modèle de service d'IP

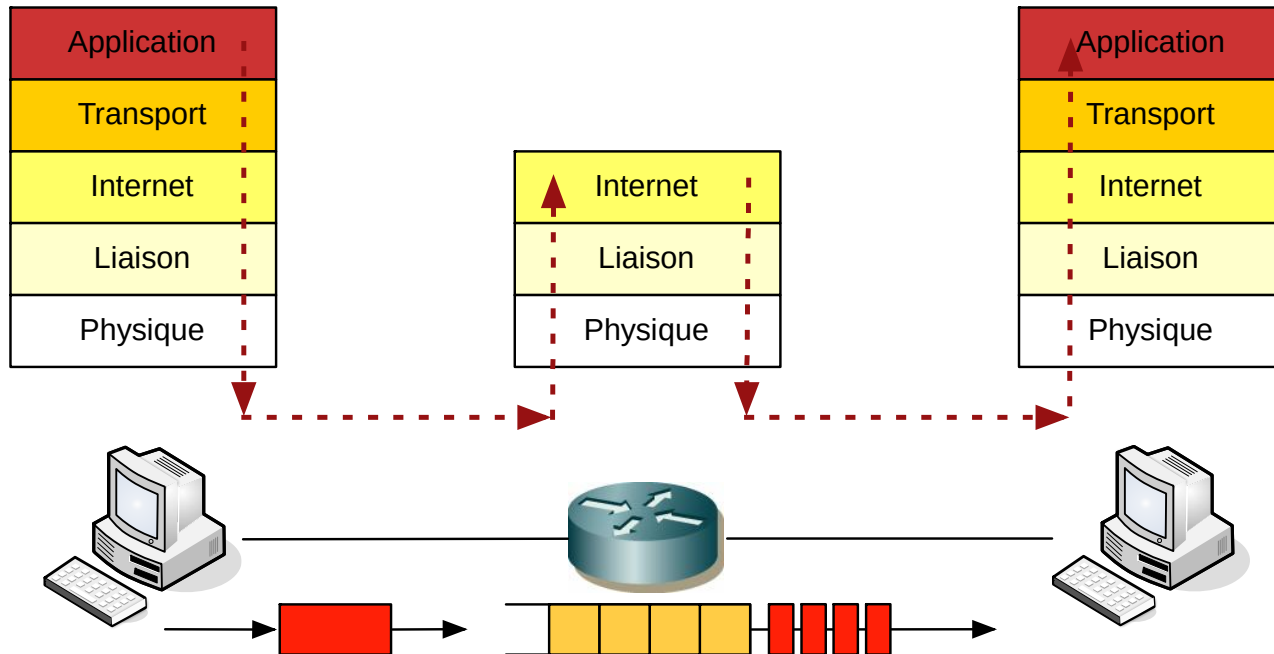


Service Best Effort

- Le routeur place les paquets dans une file d'attente
- La file d'attente entraîne des retards variables
- Si la file d'attente déborde, le paquet est perdu
- IP ne donne donc pas de garantie quant aux délais, pertes, ordre des paquets



Modèle de service d'IP

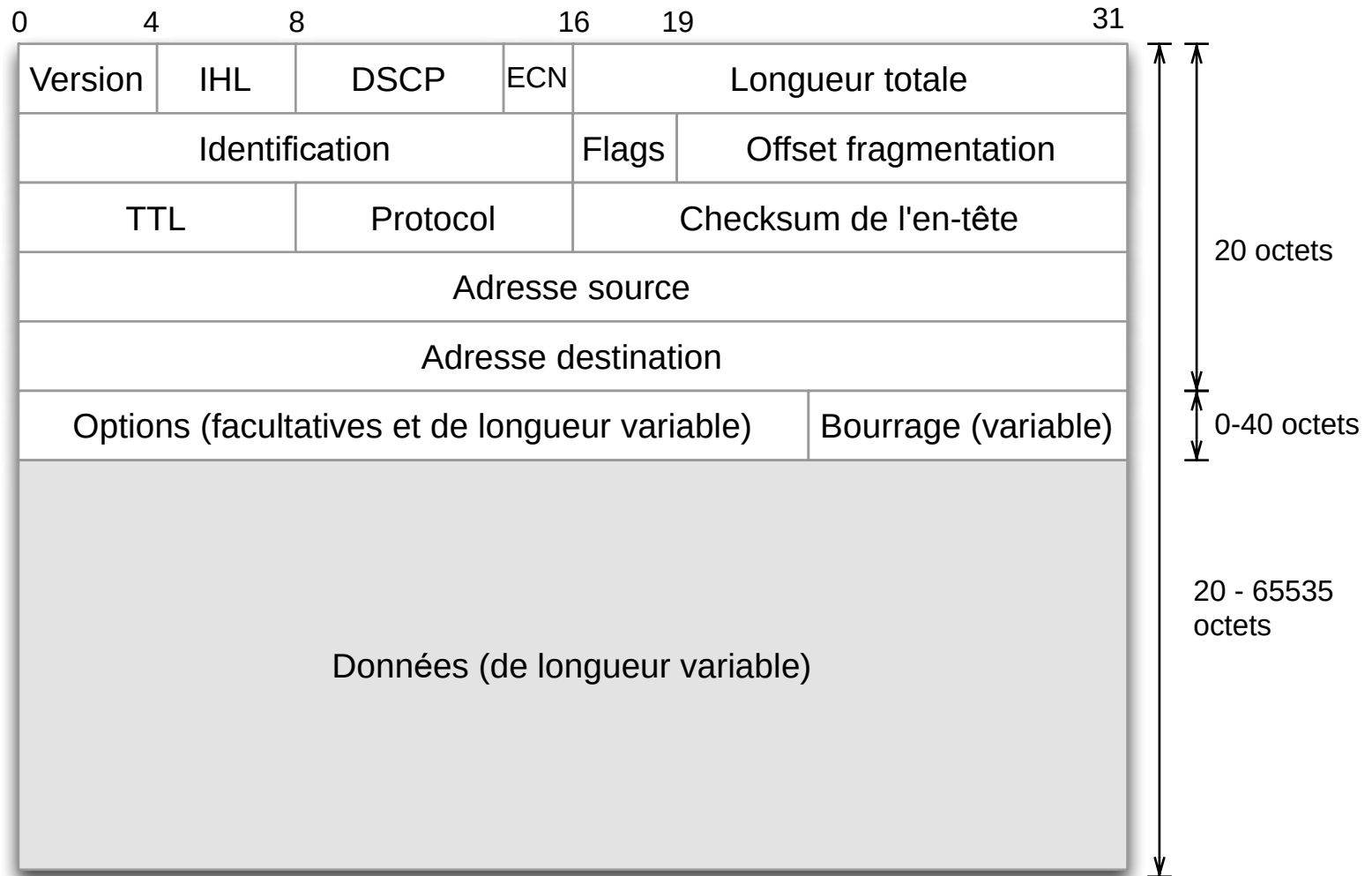


Fragmentation et réassemblage

- Si le datagramme est trop grand pour l'interface, le routeur le fragmente et transmet les fragments séparément
- Le destinataire final réassemble le datagramme originale



Format des datagrammes IP (v4)



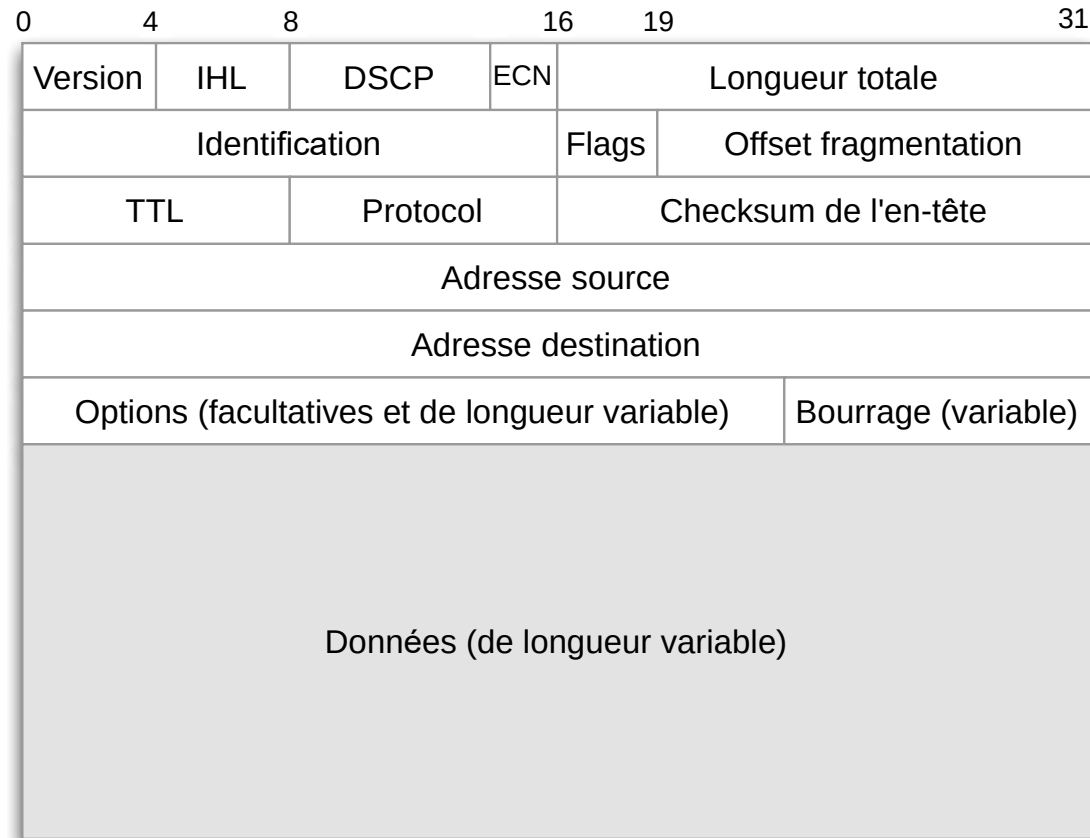
Format des datagrammes IP (v4)

Version (4 bits)

- Indique la version: IPv4 ou IPv6

IHL (4 bits)

- Internet Header Length*
- Longueur de l'en-tête
- Nécessaire à cause des options
- En multiples de 4 octets
 - IHL = 5 → 20 octets
- L'en-tête a une longueur de 20 – 60 octets



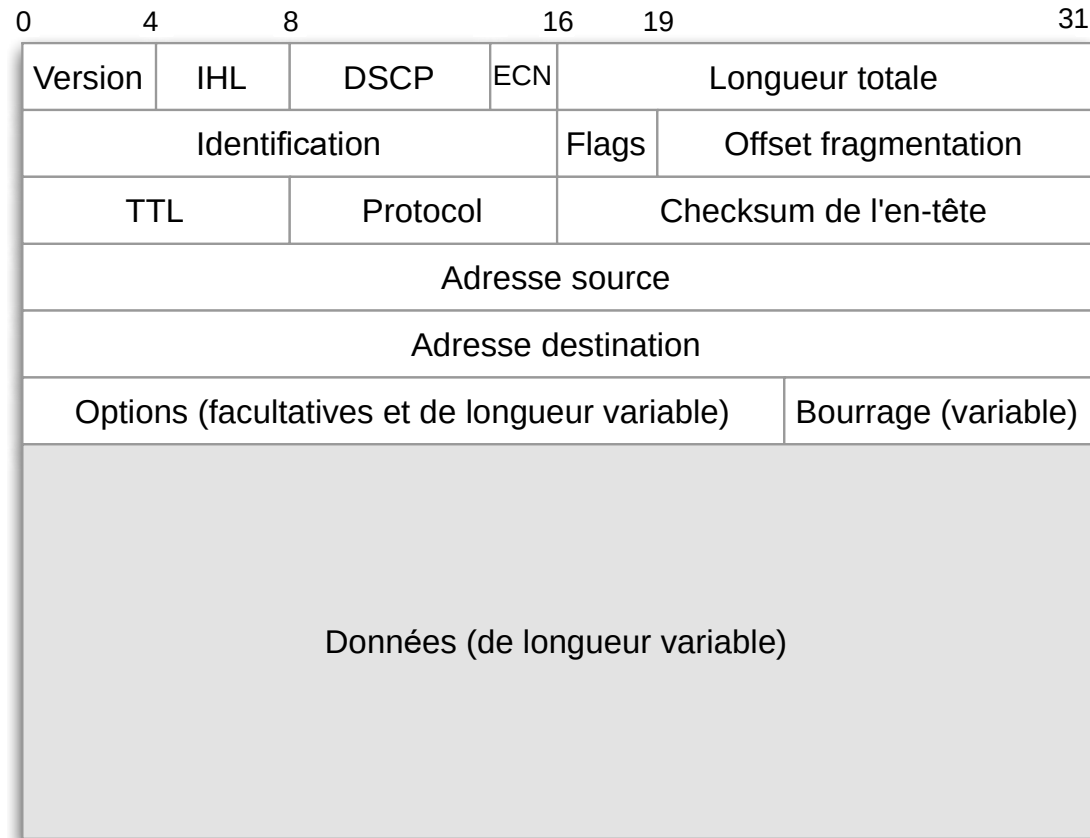
Format des datagrammes IP (v4)

DSCP (6 bits)

- Rarement utilisé
- Permet de définir des qualités de service
- Exemple : service avec débit garanti

ECN (2 bits)

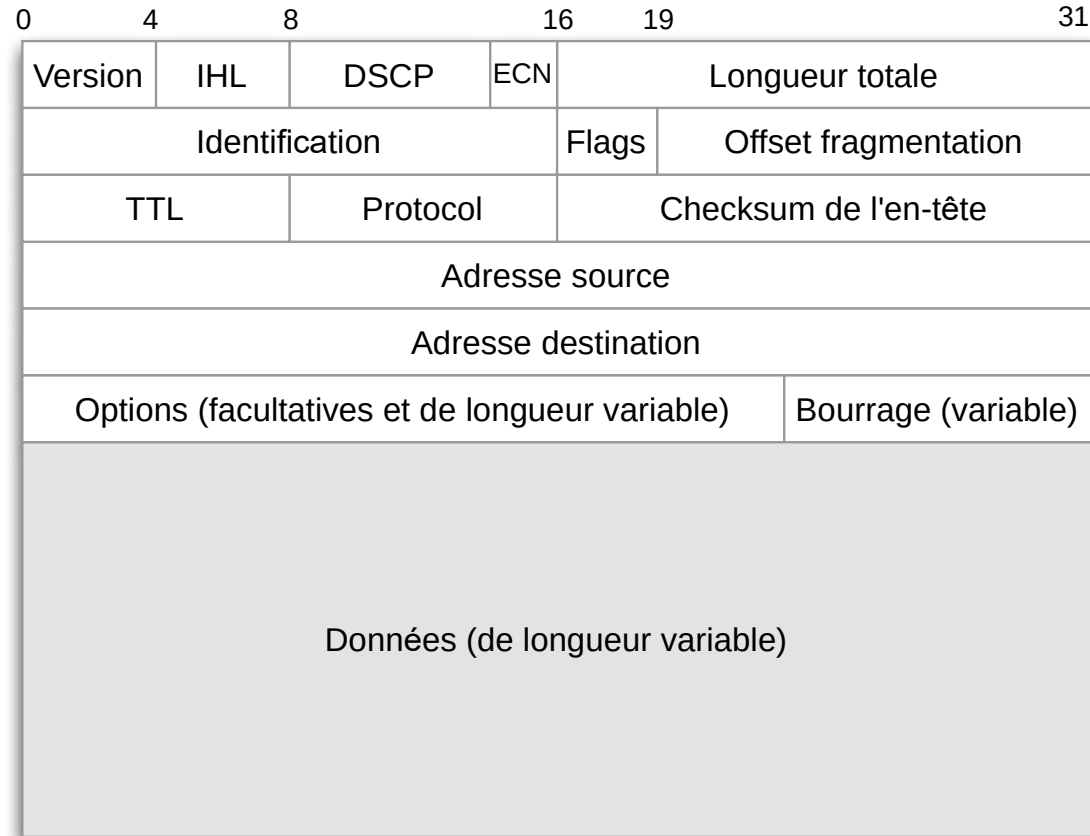
- *Explicit congestion notification*
- Extension récente et avancée qui permet aux routeurs de signaler une congestion à une source
- Cette fonction est de plus en plus utilisé par les OS



Format des datagrammes IP (v4)

Longueur totale (16 bits)

- Indique la longueur totale du datagramme, en octets
- Longueur maximale : 65'535 octets



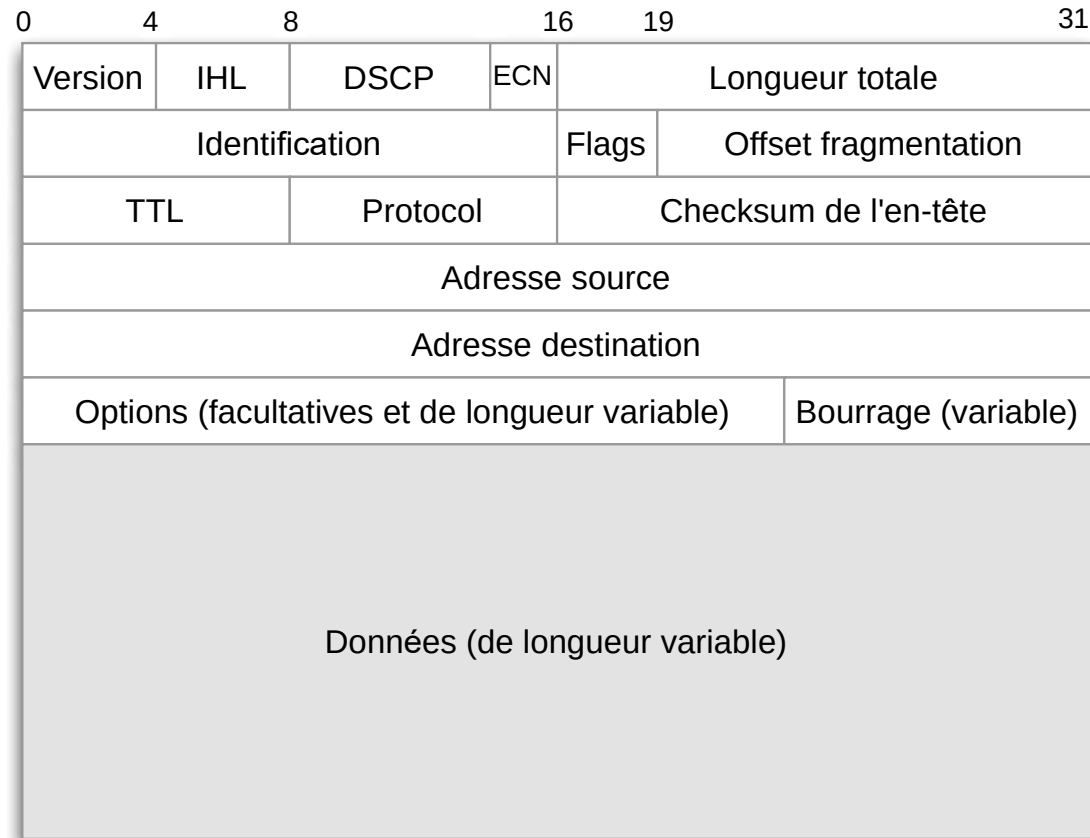
Format des datagrammes IP (v4)

Identification (16 bits)

Flags (3 bits)

Offset de fragmentation

- Utilisés pour la fragmentation et le réassemblage de datagrammes



Format des datagrammes IP (v4)

TTL (8 bits)

- Time-to-live
- Permet d'éliminer des paquets pris dans une boucle de routage
- Le champ est décrémenté par chaque routeur
- Le paquet est éliminé si le compteur atteint 0

Protocole (8 bits)

- Indique le protocole de la couche supérieure
- Indique à qui IP doit passer les données du paquet

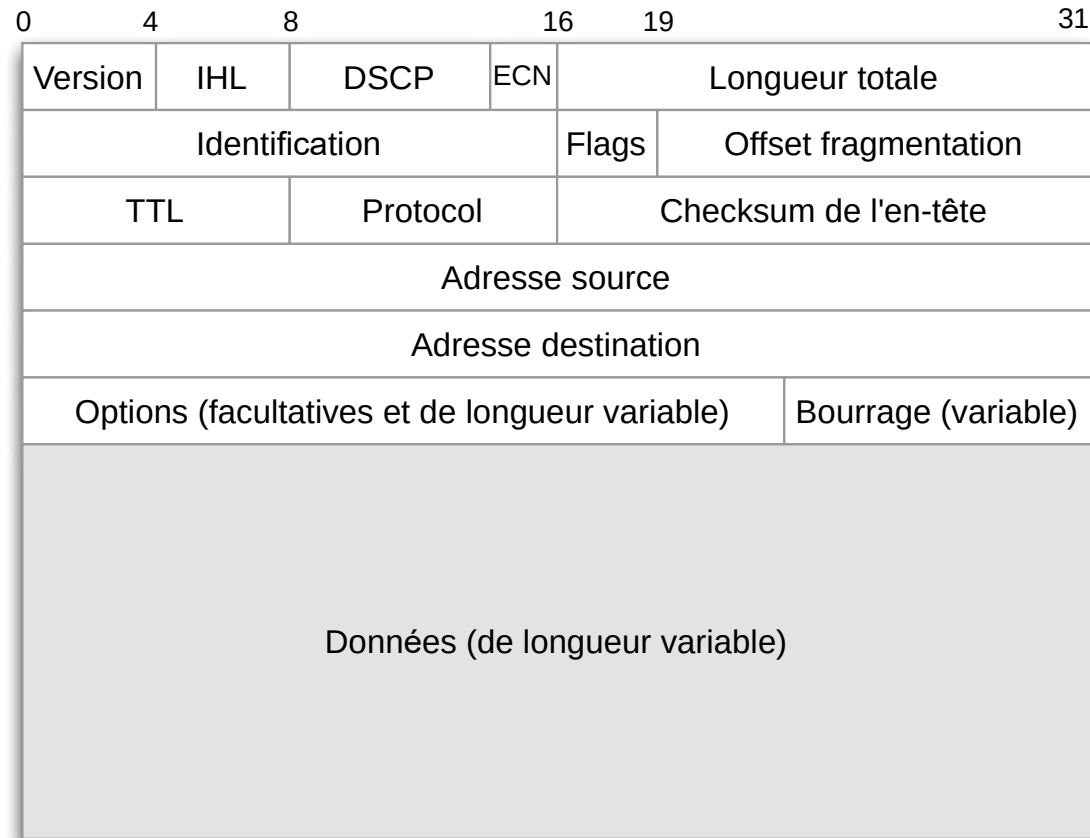
0	4	8	16	19	31
Version	IHL	DSCP	ECN	Longueur totale	
Identification			Flags	Offset fragmentation	
TTL		Protocol		Checksum de l'en-tête	
Adresse source					
Adresse destination					
Options (facultatives et de longueur variable)				Bourrage (variable)	
Données (de longueur variable)					



Format des datagrammes IP (v4)

Checksum de l'en-tête (16 bits)

- Somme de contrôle qui peut détecter des erreurs de bit dans l'en-tête (pas dans les données)
- Chaque routeur la vérifie et écarte les paquets erronés
- Comme le TTL change à chaque saut, chaque routeur doit mettre à jour cette somme de contrôle

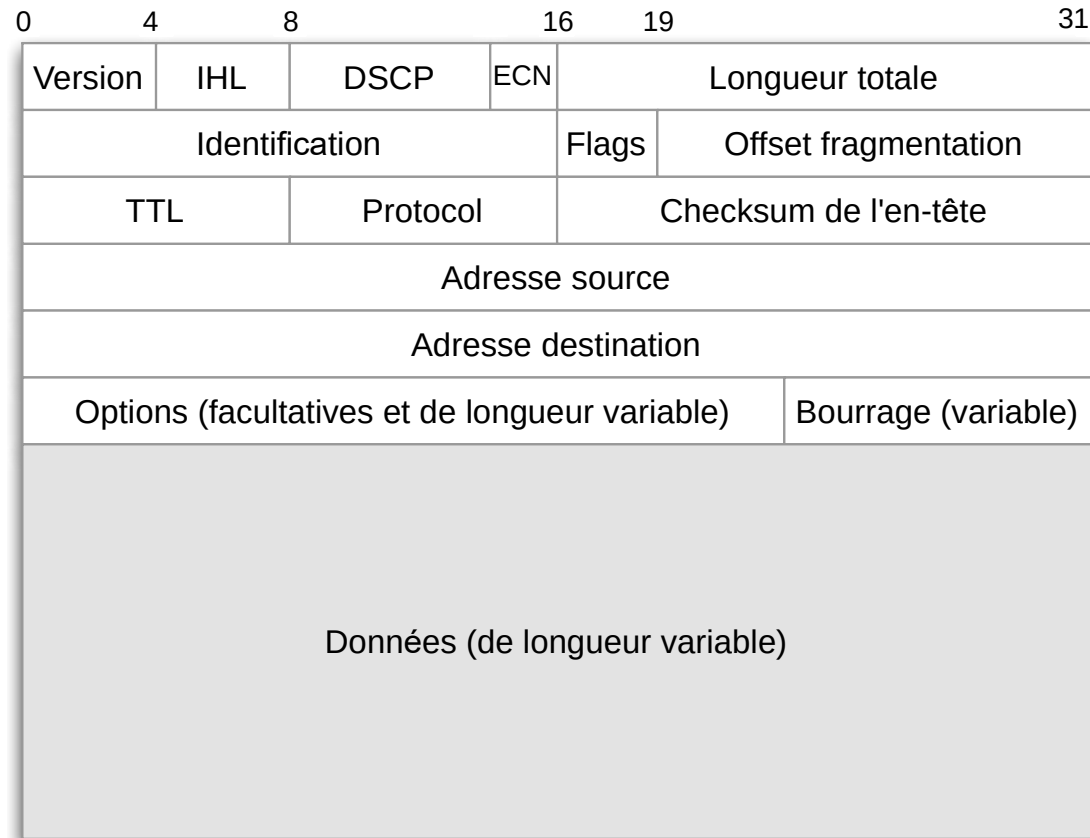


Format des datagrammes IP (v4)

Adresse source

Adresse destination

- Adresses IPv4 des terminaux sur 32 bits



Format des datagrammes IP (v4)

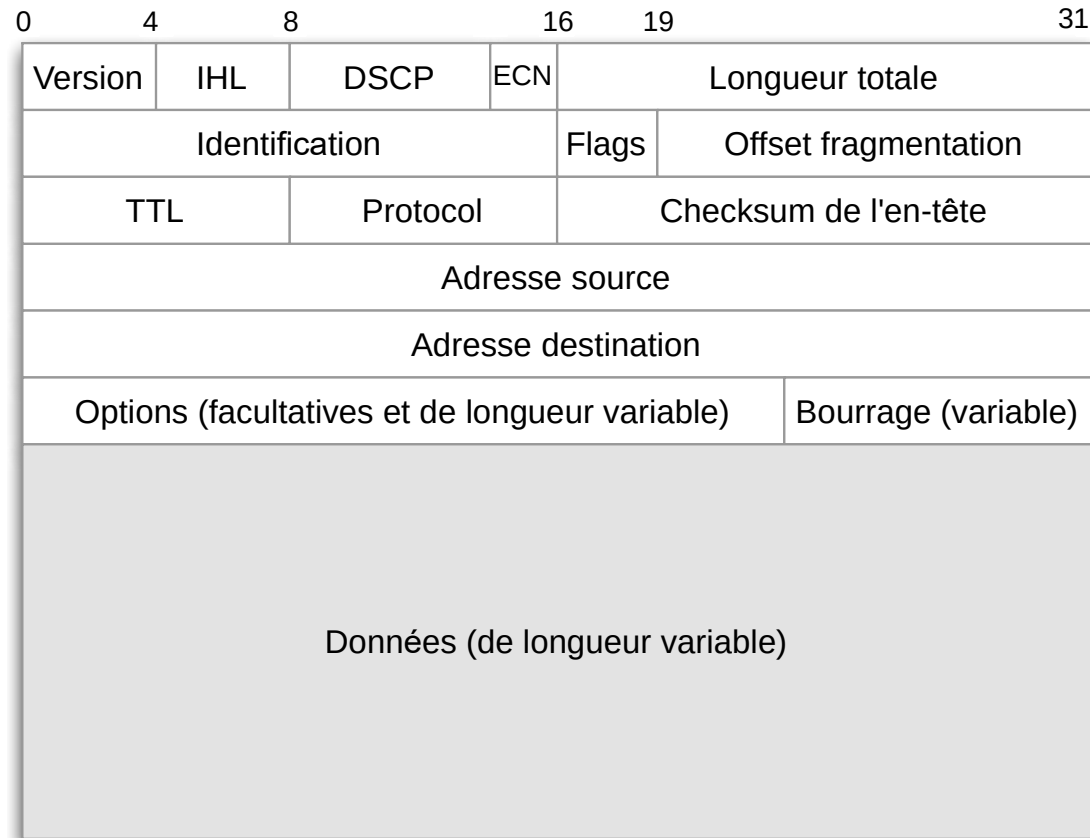
Options (longueur variable)

- Rarement utilisées
- Par exemple options de routage, sécurité

Bourrage

(longueur variable)

- La longueur de l'en-tête doit être un multiple de 4 octets
- Si nécessaire, le bourrage rallonge l'en-tête de 1-3 octets

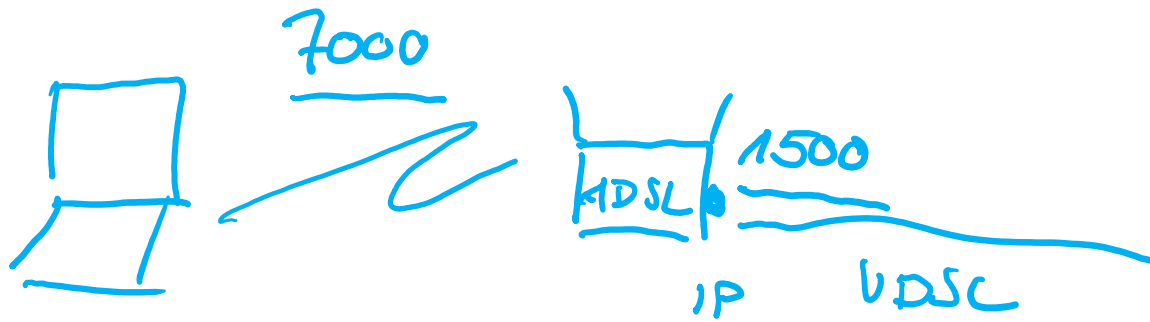


Fragmentation et réassemblage

- Un routeur (ou la source) fragmente un datagramme s'il est trop long pour l'interface
 - Ethernet: 1500 octets
 - WLAN: 7981 octets
- Chaque fragment est un datagramme complet
 - Les fragments sont acheminés de manière indépendante
 - Ils peuvent être fragmentés de nouveau plus loin
- Le destinataire doit réassembler les fragments
 - Les fragments peuvent arriver en désordre
 - Si un fragment est perdu, le datagramme sera supprimé



Fragmentation et réassemblage



Fragmentation et réassemblage

- Un routeur (ou la source) fragmente un datagramme s'il est trop long pour l'interface
 - Ethernet: 1500 octets
 - WLAN: 7981 octets
- Chaque fragment est un datagramme complet
 - Les fragments sont acheminés de manière indépendante
 - Ils peuvent être fragmentés de nouveau plus loin
- Le destinataire doit réassembler les fragments
 - Les fragments peuvent arriver en désordre
 - Si un fragment est perdu, le datagramme sera supprimé



Fragmentation et réassemblage

- Identification

- Identificateur unique d'un datagramme
- Permet de reconnaître les fragments

- Flags

- DF: Don't fragment
 - Mis par la source
 - Empêche la fragmentation
- MF: More fragments
 - 0 pour le dernier fragment, sinon 1

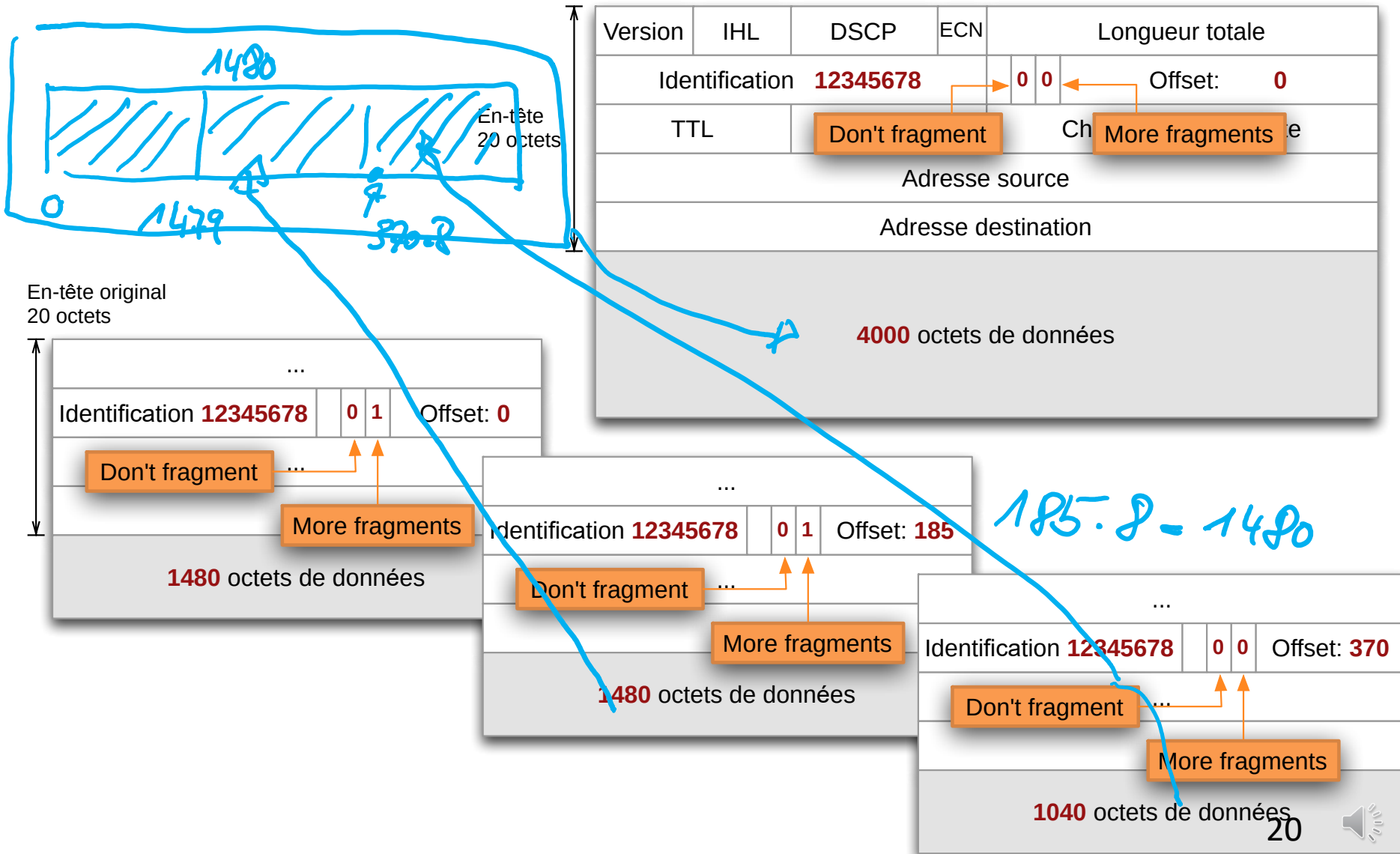
- Offset

- Position du fragment dans le datagramme
- En multiples de 8 octets

0	4	8	16	19	31
Version	IHL	DSCP	ECN	Longueur totale	
Identification			Flags	Offset fragmentation	
TTL		Protocol		Checksum de l'en-tête	
Adresse source					
Adresse destination					
Options (facultatives et de longueur variable)				Bourrage (variable)	



Fragmentation



Fin du chapitre 5

