Téléinformatique de base

Chapitre 5

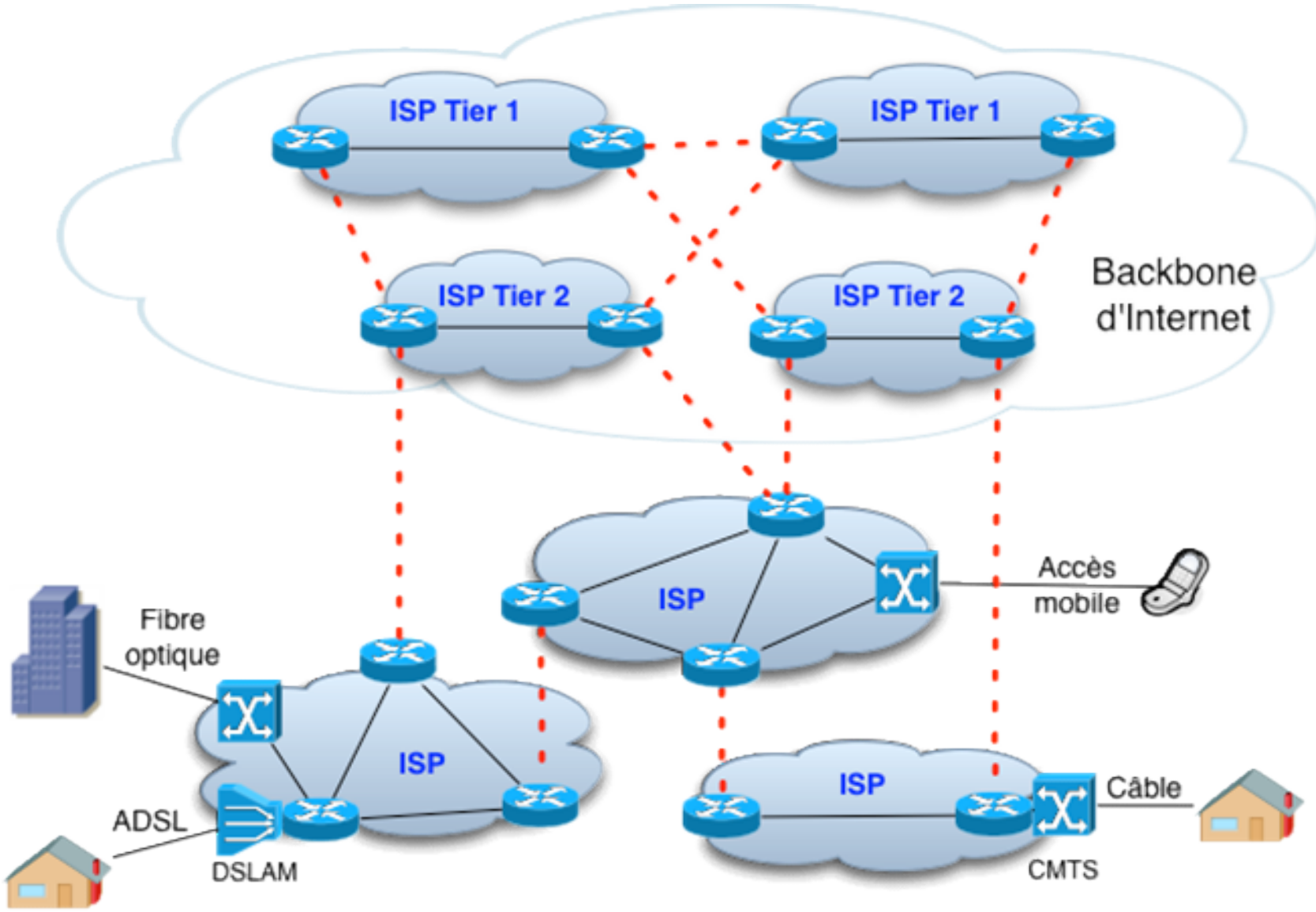
Les réseaux IP

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Objectifs d'apprentissage

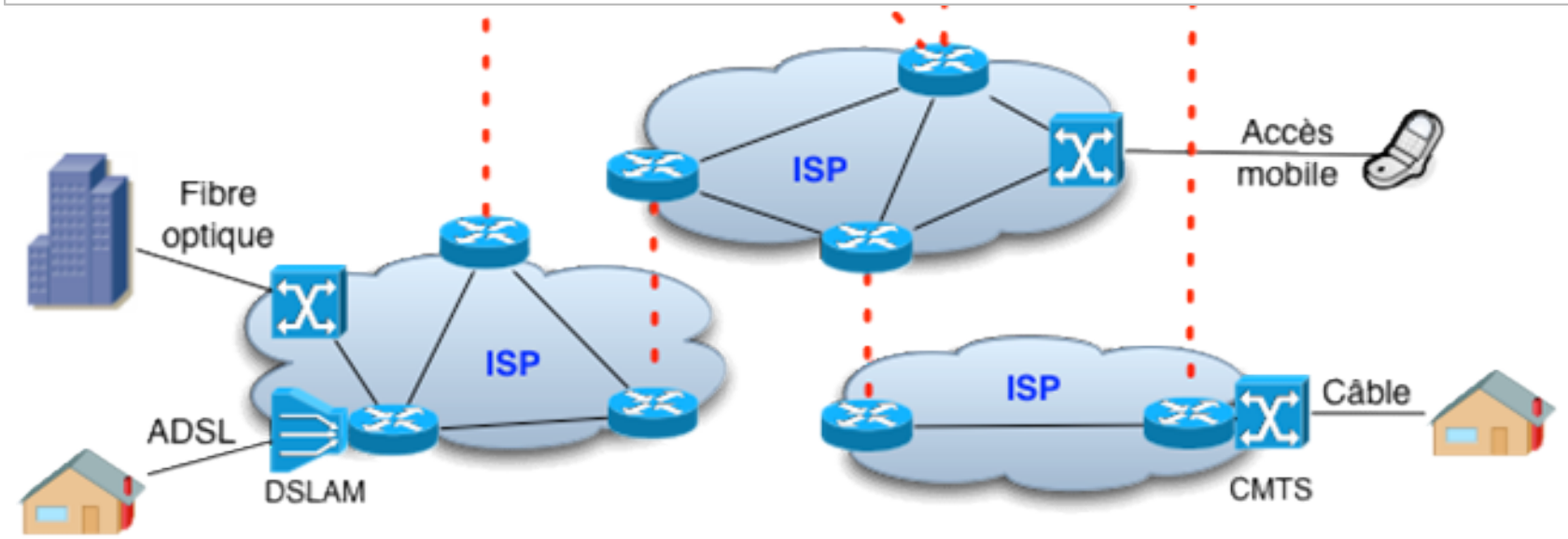
- Savoir expliquer la structure d'Internet, notamment l'interconnexion des réseaux.
- Savoir expliquer les mécanismes du protocole IP
- Savoir calculer des plages d'adresses pour un masque de sous-réseaux
- Savoir distinguer des plages d'adresses privées
- Savoir expliquer le fonctionnement de NAT et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

Architecture d'Internet

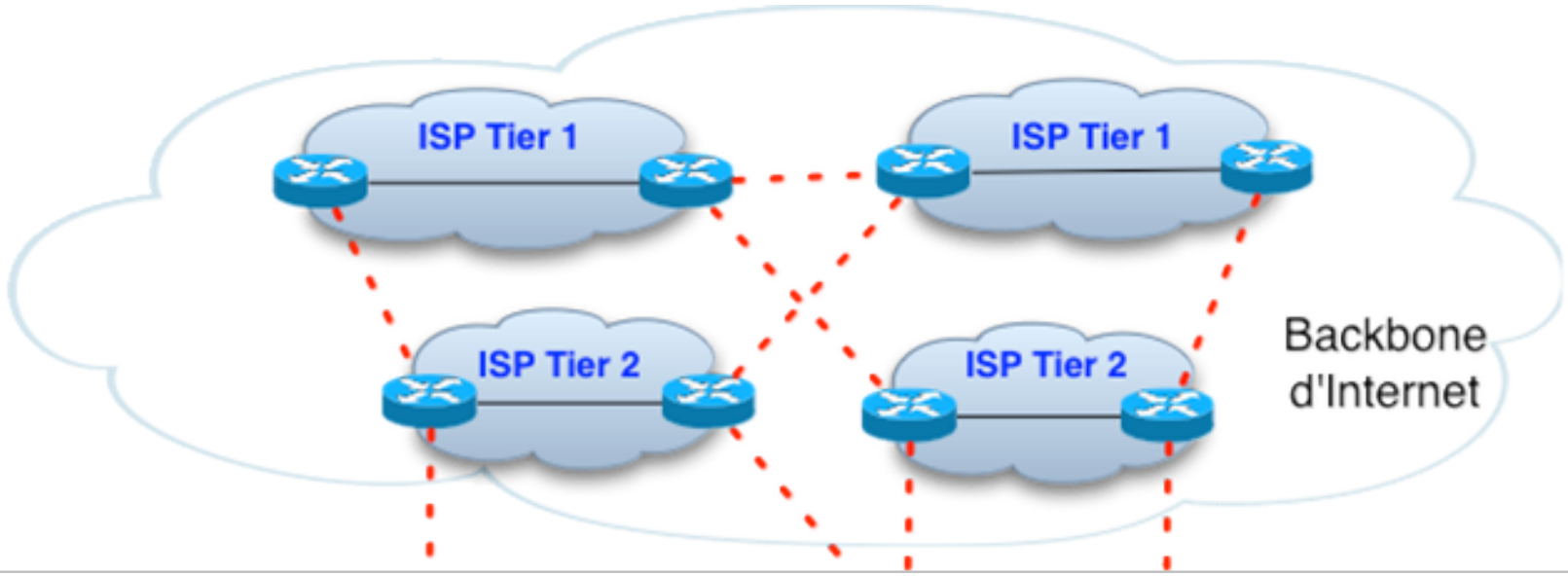


Architecture d'Internet

- Les utilisateurs (particuliers, entreprises et organisations) sont connectés à Internet par un ISP (Internet Service Provider)
- Les technologies typiques sont
  - xDSL (ADSL, VDSL, typiquement 1 – 20 Mb/s)
  - Modem câble (typiquement 1 – 100 Mb/s)
  - Accès mobile (3G ou LTE, typiquement 1 Mb/s – 100 Mb/s)
  - Fibre optique avec Ethernet (typiquement 100 Mb/s – 1 Gb/s)



Architecture d'Internet

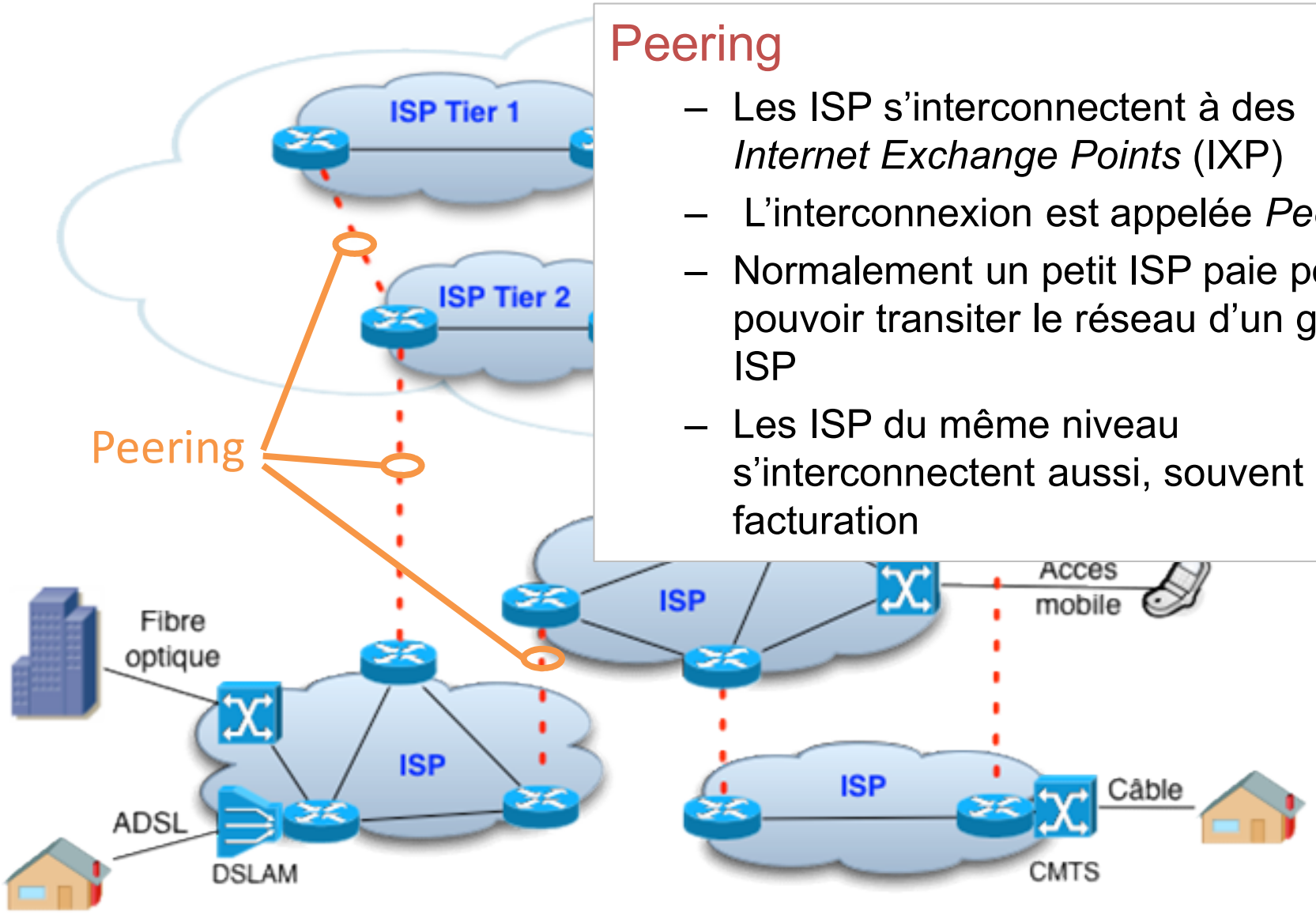


- D'autres ISP (tier 2 et tier 1) fournissent des connexions internationales et intercontinentales
- Les ISP tier 2 et tier 1 forment l'épine dorsale (Backbone) d'Internet
  - 10 – 20 ISP tier 1 en total, par exemple Level3, Deutsche Telekom, Sprint
- Ces ISP utilisent principalement des fibres optiques à longue distance, avec des débits jusqu'à 100 Gb/s

DSLAM

CMTS

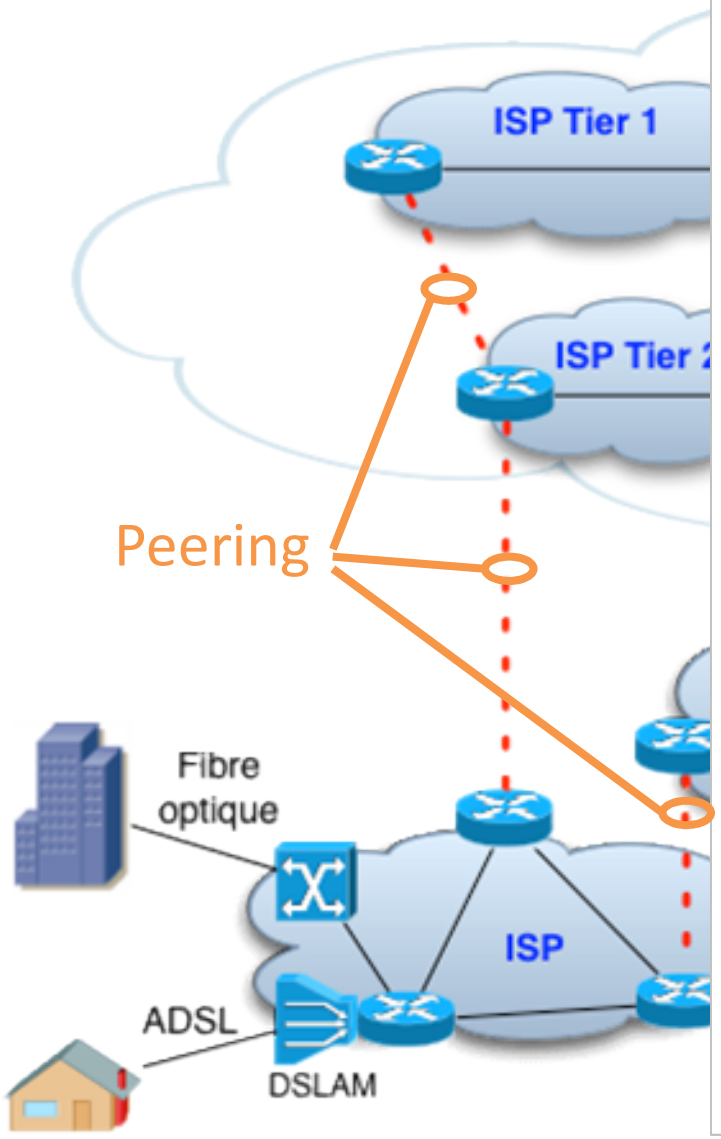
Architecture d'Internet



Peering

- Les ISP s'interconnectent à des *Internet Exchange Points* (IXP)
- L'interconnexion est appelée *Peering*
- Normalement un petit ISP paie pour pouvoir transiter le réseau d'un grand ISP
- Les ISP du même niveau s'interconnectent aussi, souvent sans facturation

Architecture d'Internet



Peering

- Un IXP est simplement une salle avec des routeurs appartenant à différents ISP
- Un LAN haute vitesse permet d'interconnecter les routeurs de deux ISP pour effectuer le peering

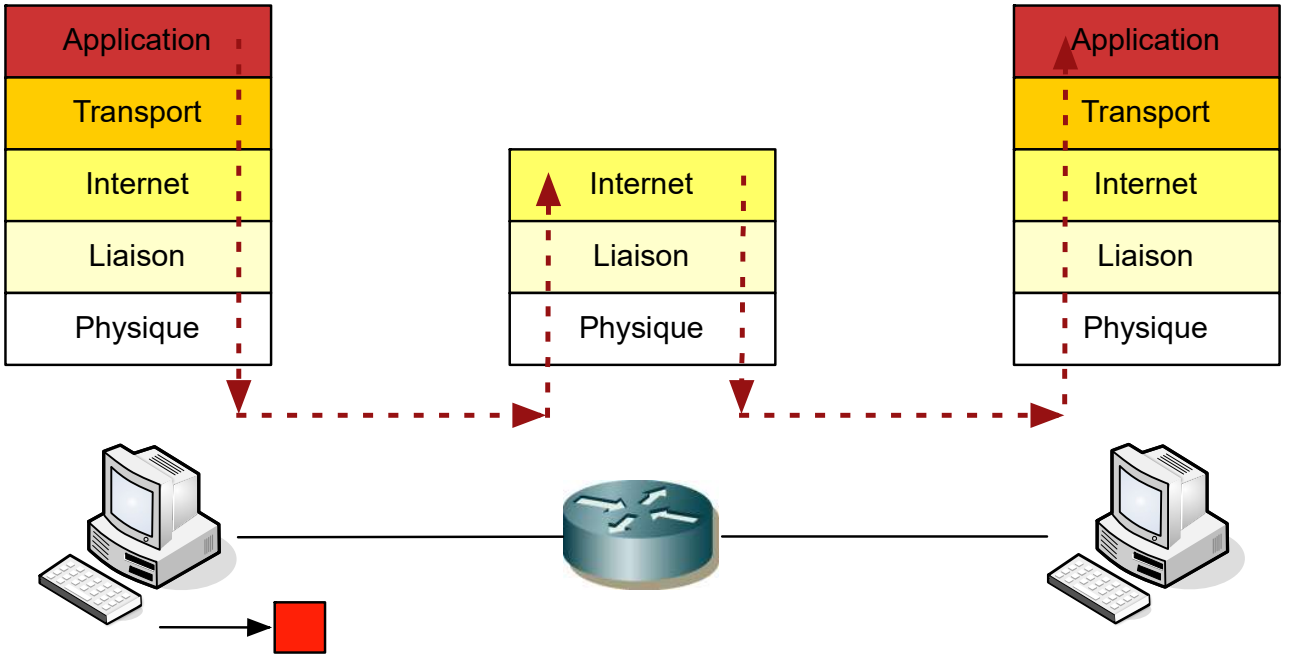
Internet Protocol (IP)

- Chaque ISP peut utiliser la technologie qui lui convient
  - Fibres optiques, liaisons hertziennes, ... comme support physique
  - Ethernet, ATM, SDH, … comme protocoles couche 1 et 2
  - RIP, OSPF, IS-IS, … comme protocole de routage
- Mais tous doivent utiliser le protocole IP comme protocole de la couche 3
- IP est le langage commun d'Internet et des réseaux informatiques
- Les terminaux et les routeurs des réseaux utilisent IP pour transporter les données

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

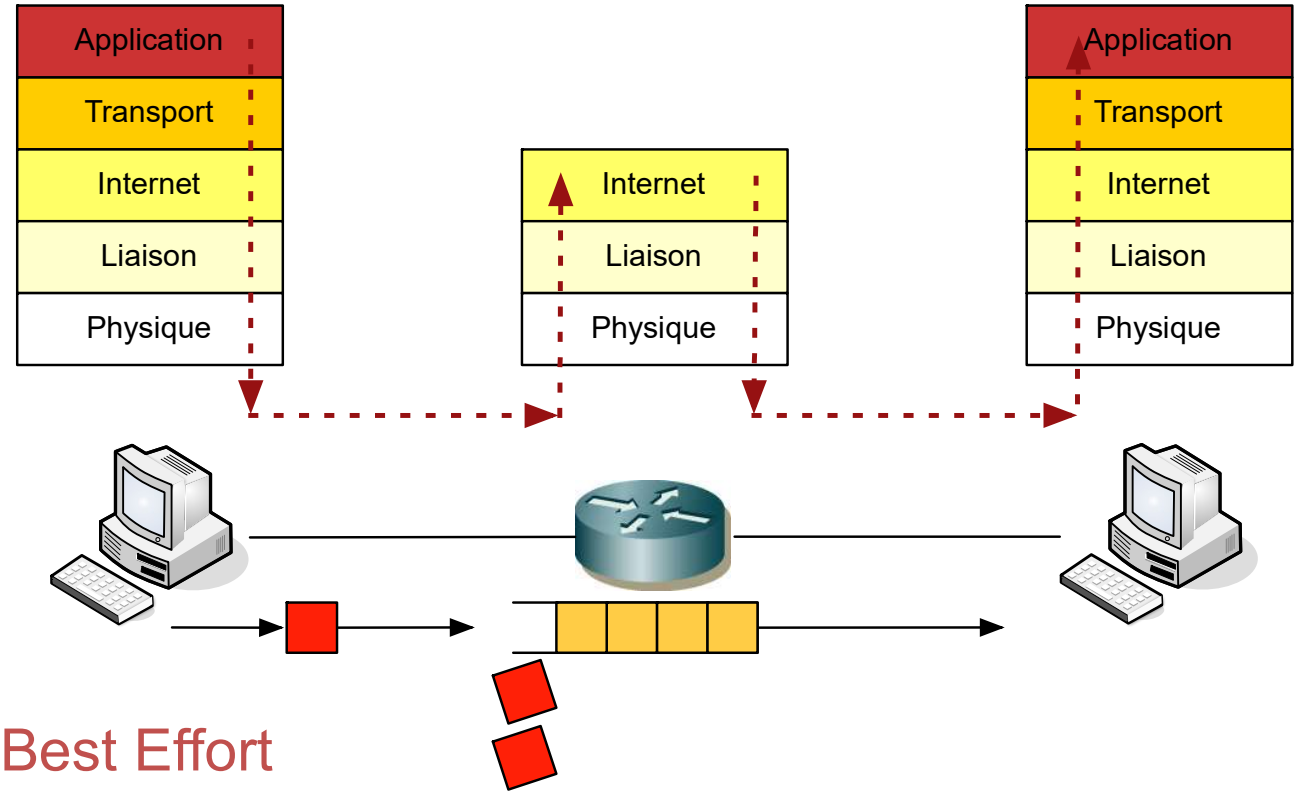
Modèle de service d'IP



Sans connexion

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

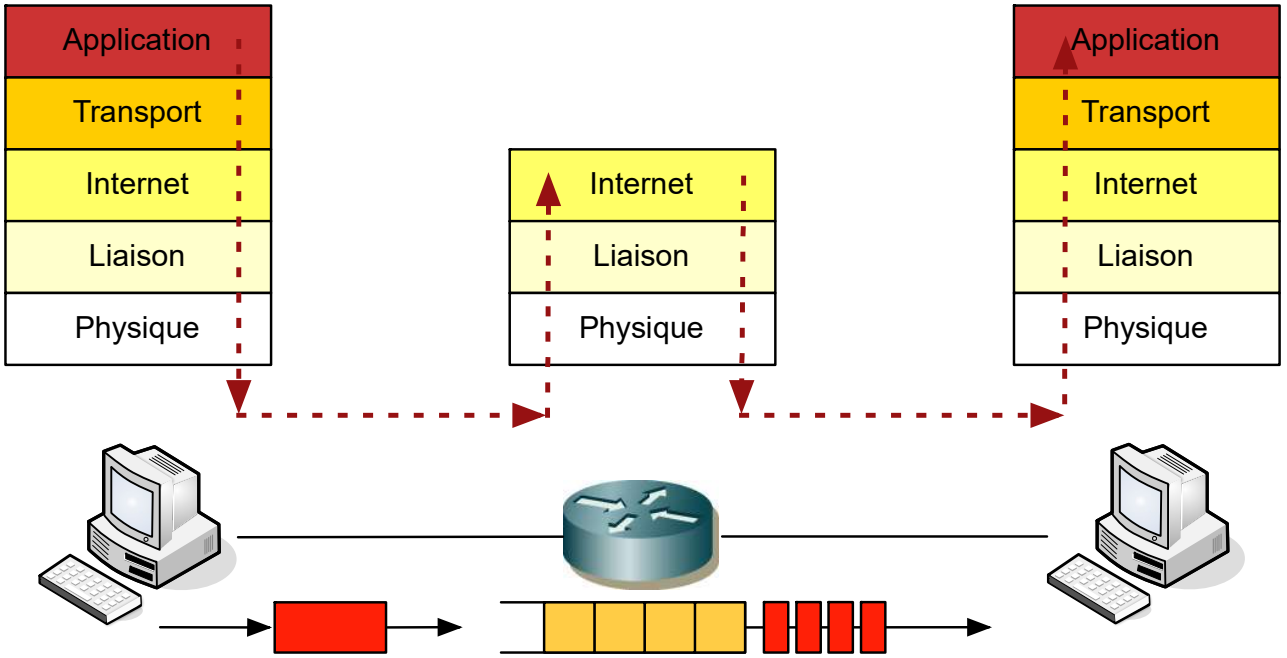
Modèle de service d'IP



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

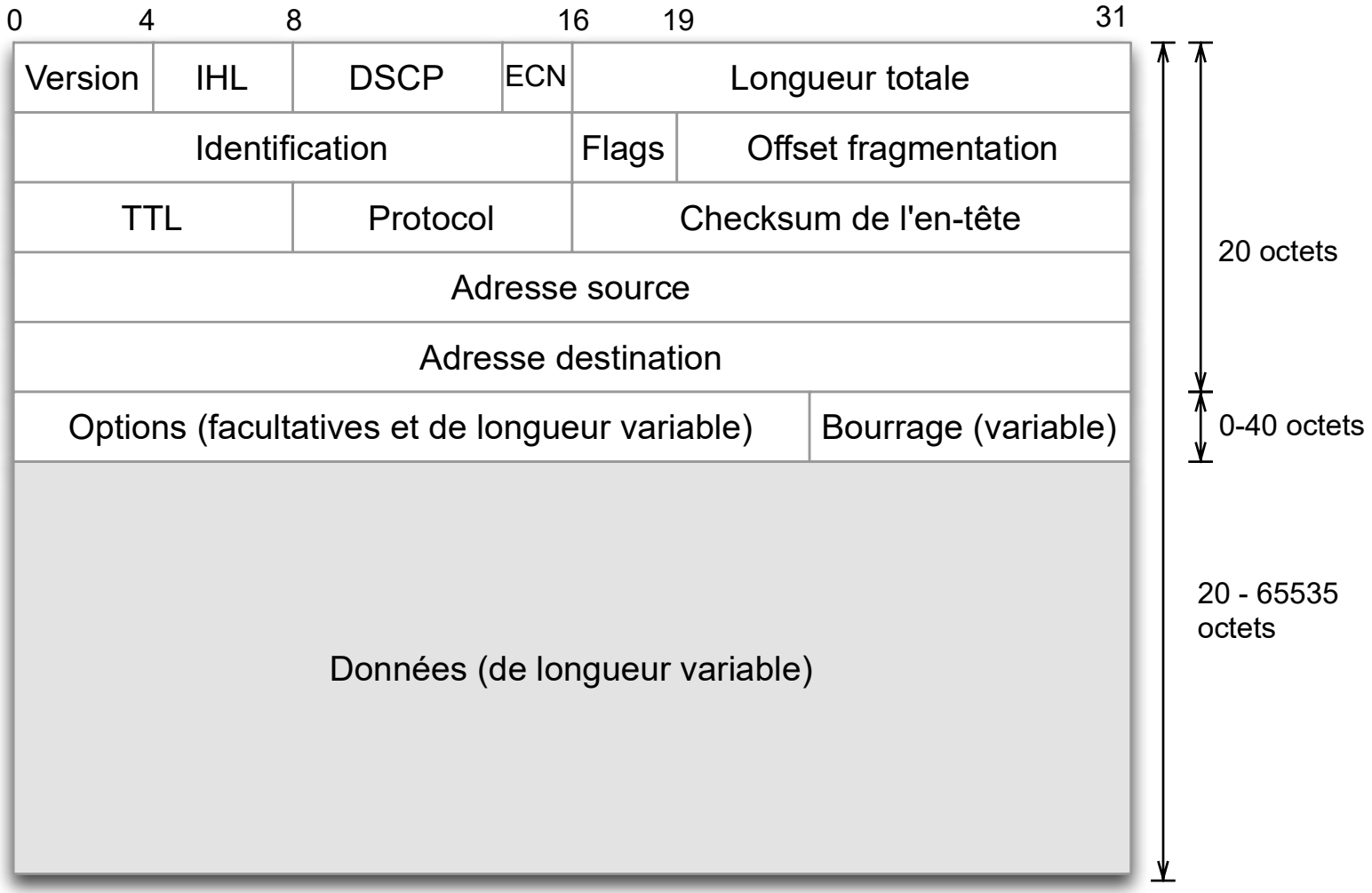
Modèle de service d'IP



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)



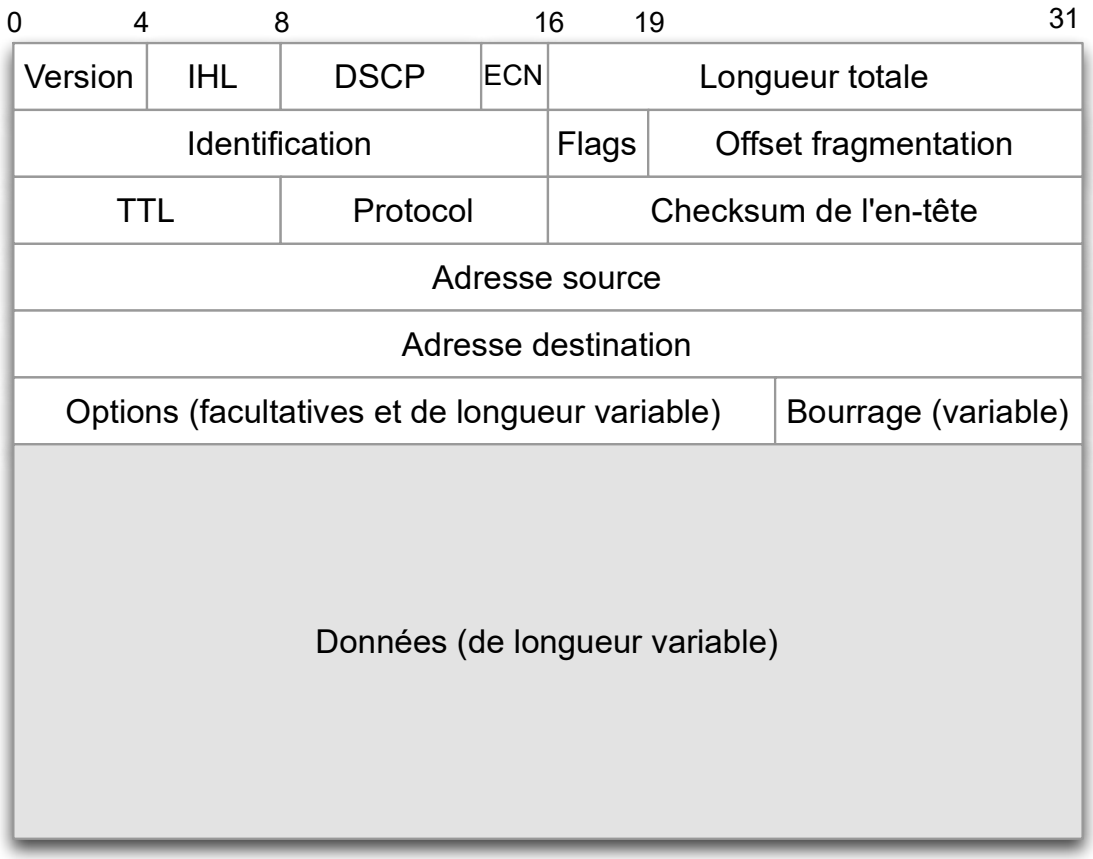
Format des datagrammes IP (v4)

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



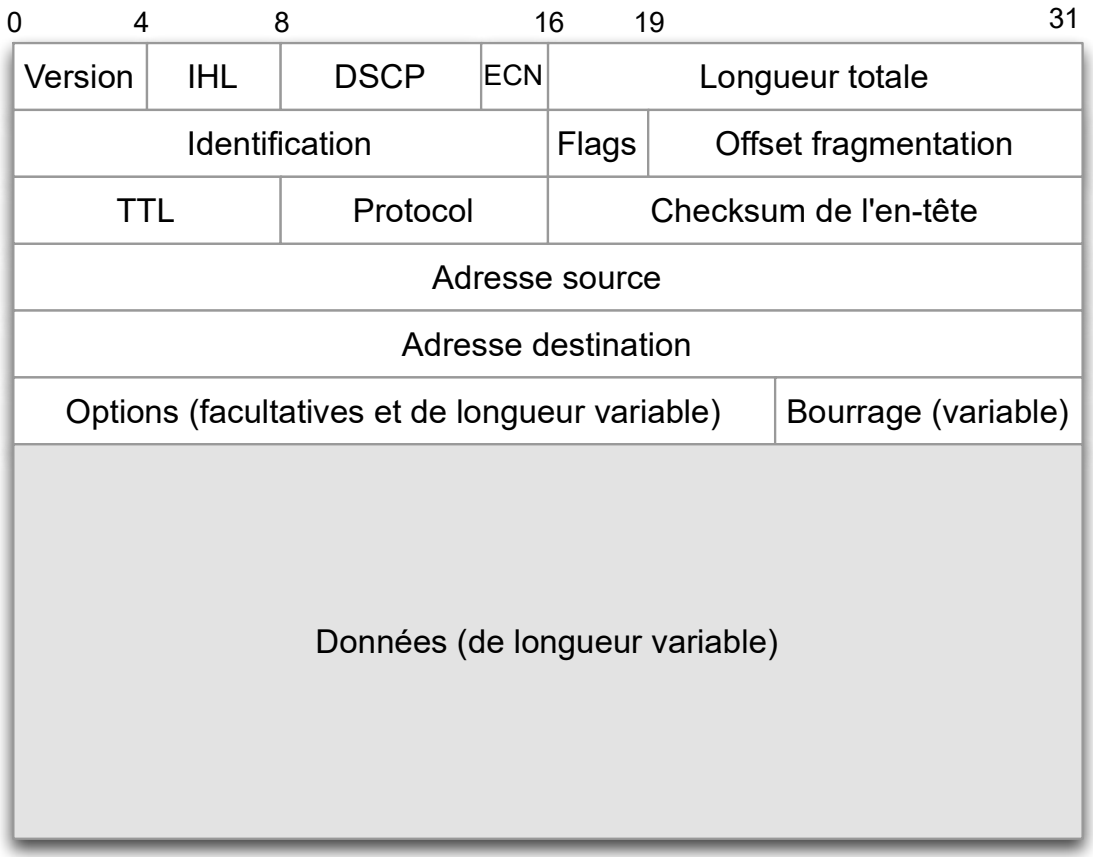
Format des datagrammes IP (v4)

DSCP (6 bits)

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

ECN (2 bits)

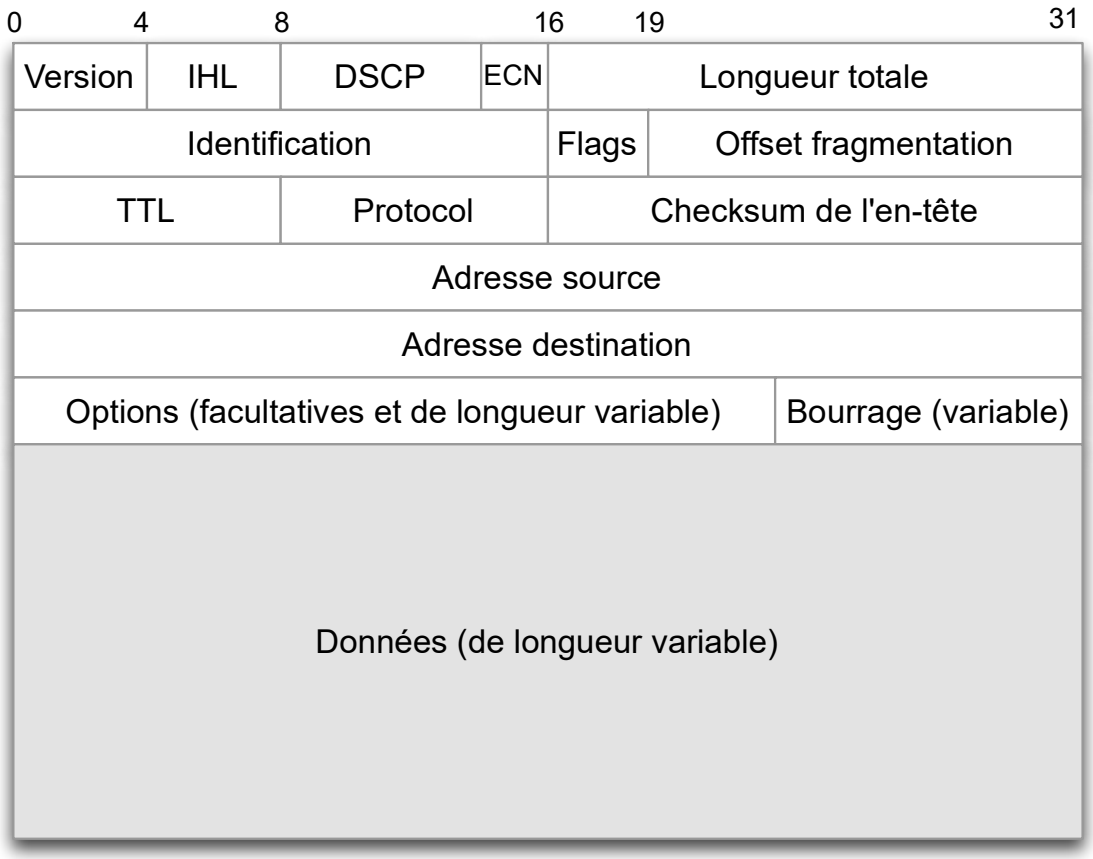
- *Explicit congestion notification*
- Extension récente et avancée qui permet aux routeurs de signaler une congestion à une source
- Cette fonction est souvent désactivé dans les OS



Format des datagrammes IP (v4)

Longueur totale (16 bits)

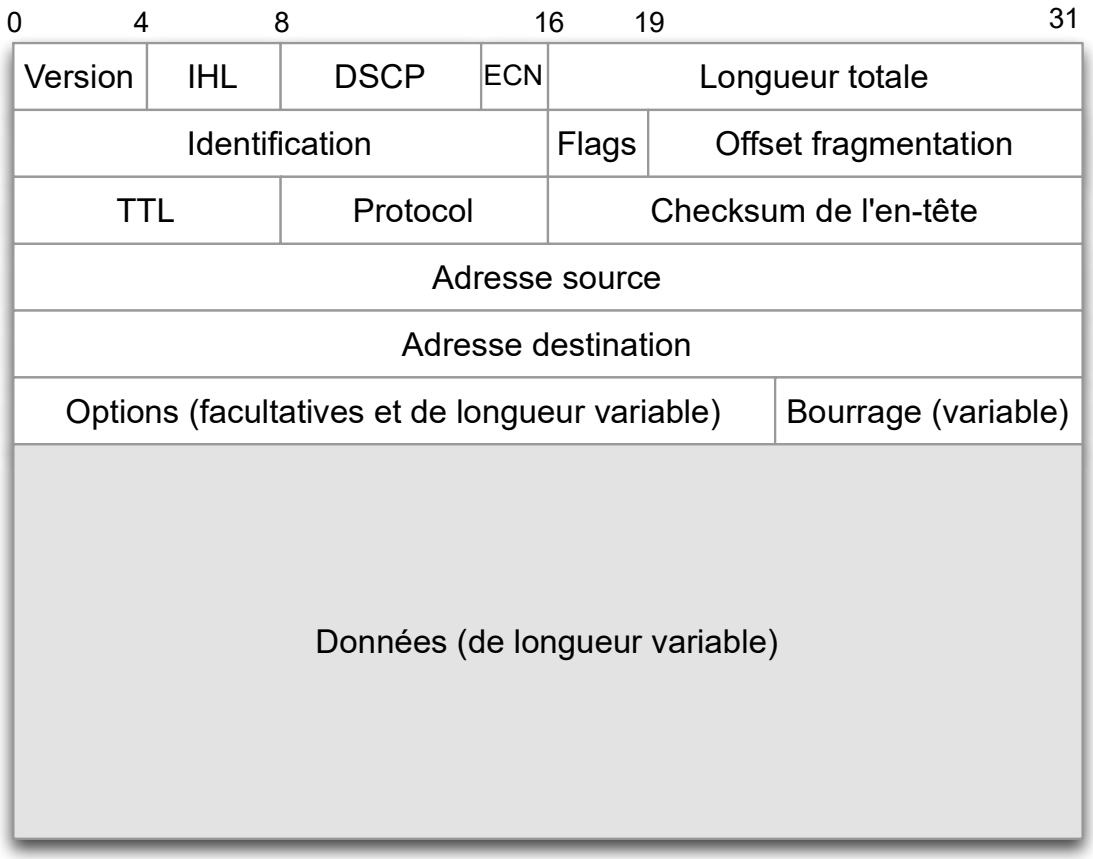
- Indique la longueur totale du datagramme, en octets
- Longueur maximale : 65’535 octets



Format des datagrammes IP (v4)

Identification (16 bits)
Flags (3 bits)
Offset de fragmentation

- Utilisés pour la fragmentation et le réassemblage de datagrammes



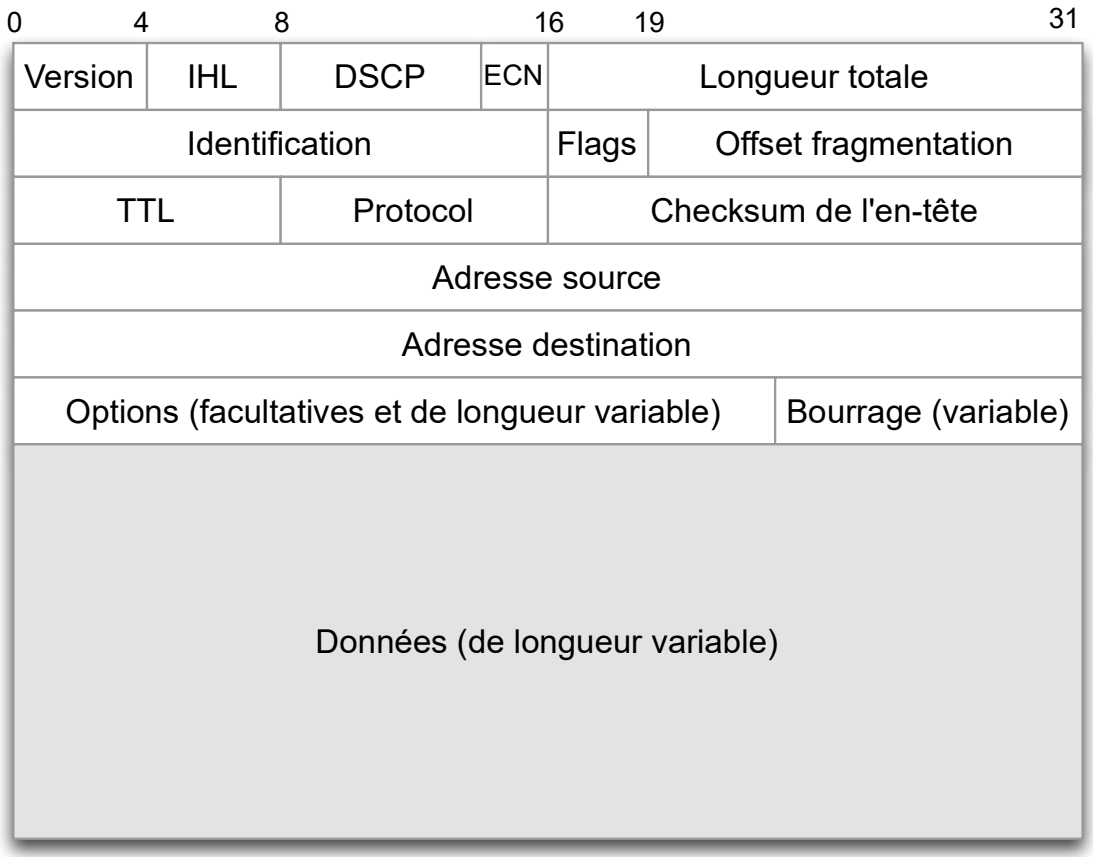
Format des datagrammes IP (v4)

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)

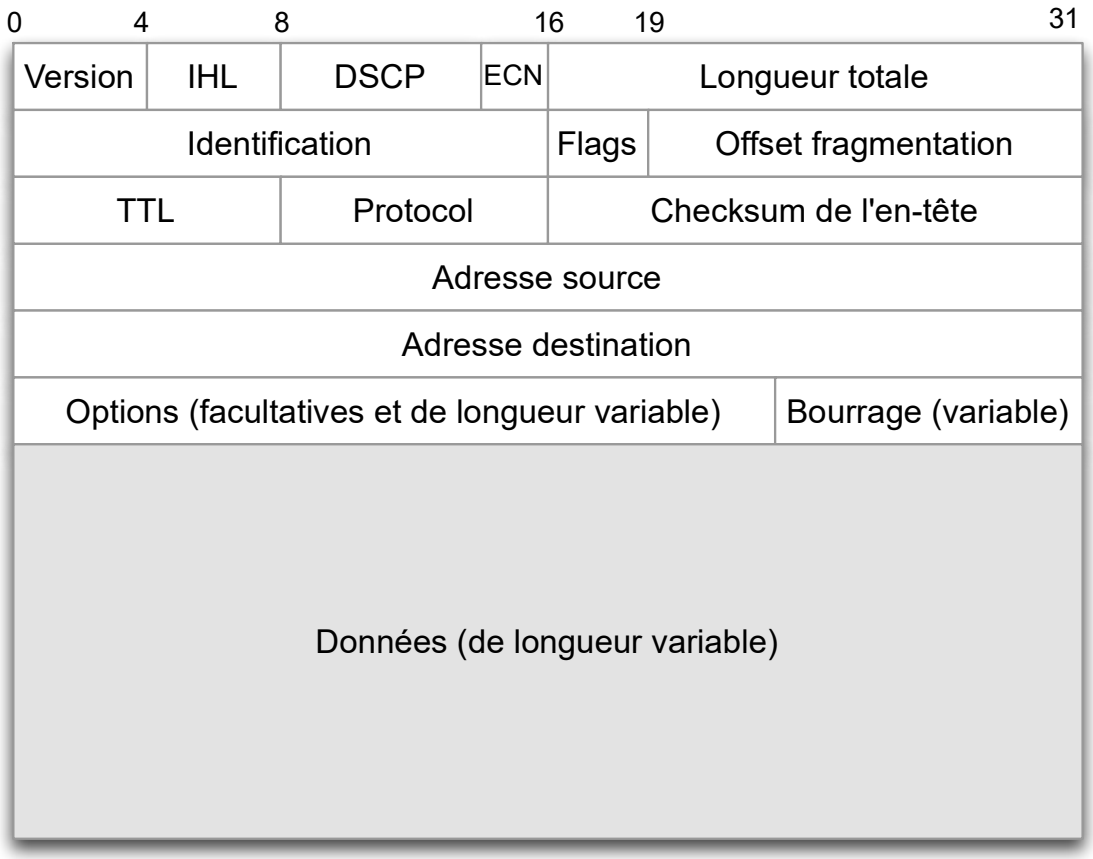
- Indique le protocole de la couche supérieure
- Indique à qui IP doit passer les données du paquet



Format des datagrammes IP (v4)

Checksum de l'en-tête (16 bits)

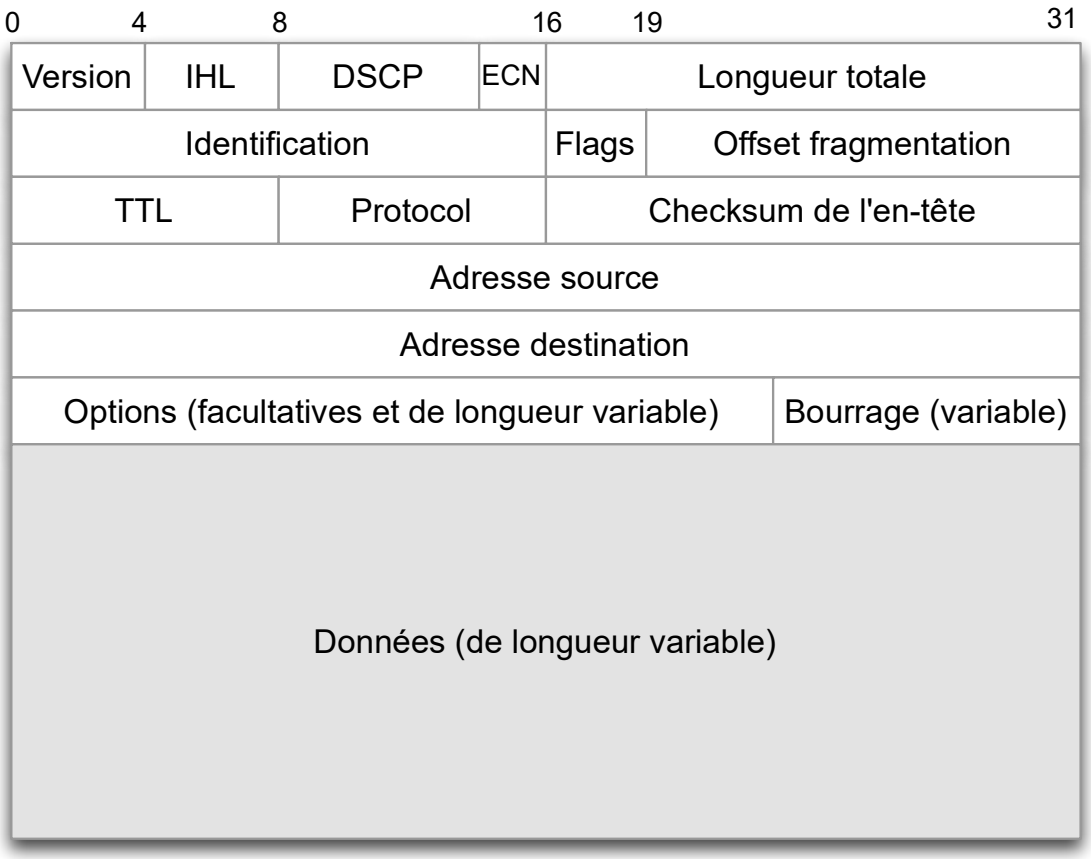
- Somme de contrôle qui peut détecter des erreurs de bit dans l'en-tête (pas dans les données)
- Chaque routeur la vérifie et écarte les paquets erronés
- Comme le TTL change à chaque saut, chaque routeur doit mettre à jour cette somme de contrôle



Format des datagrammes IP (v4)

Adresse source
Adresse destination

- Adresses IPv4 des terminaux sur 32 bits



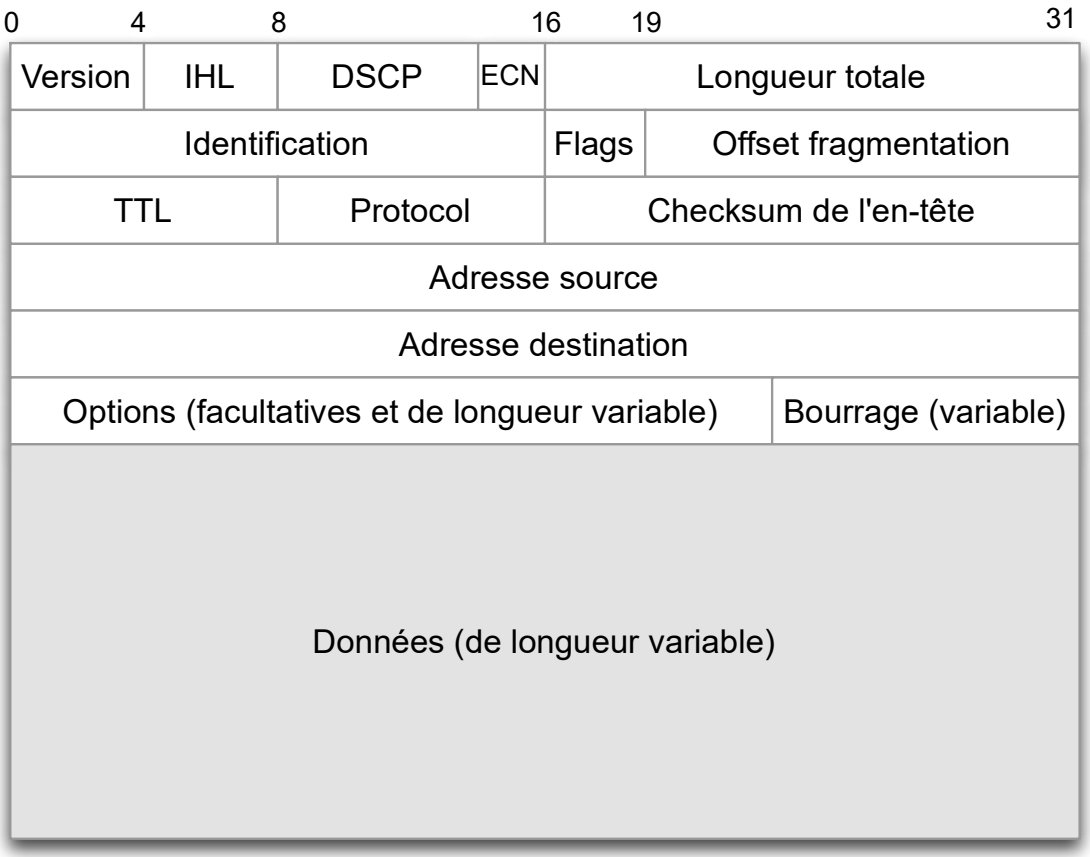
Format des datagrammes IP (v4)

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

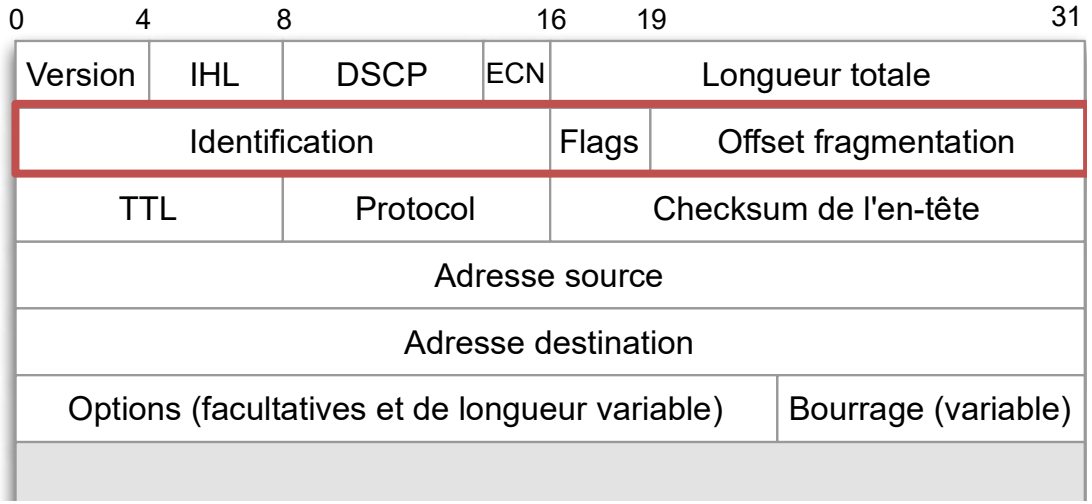


Fragmentation et réassemblage

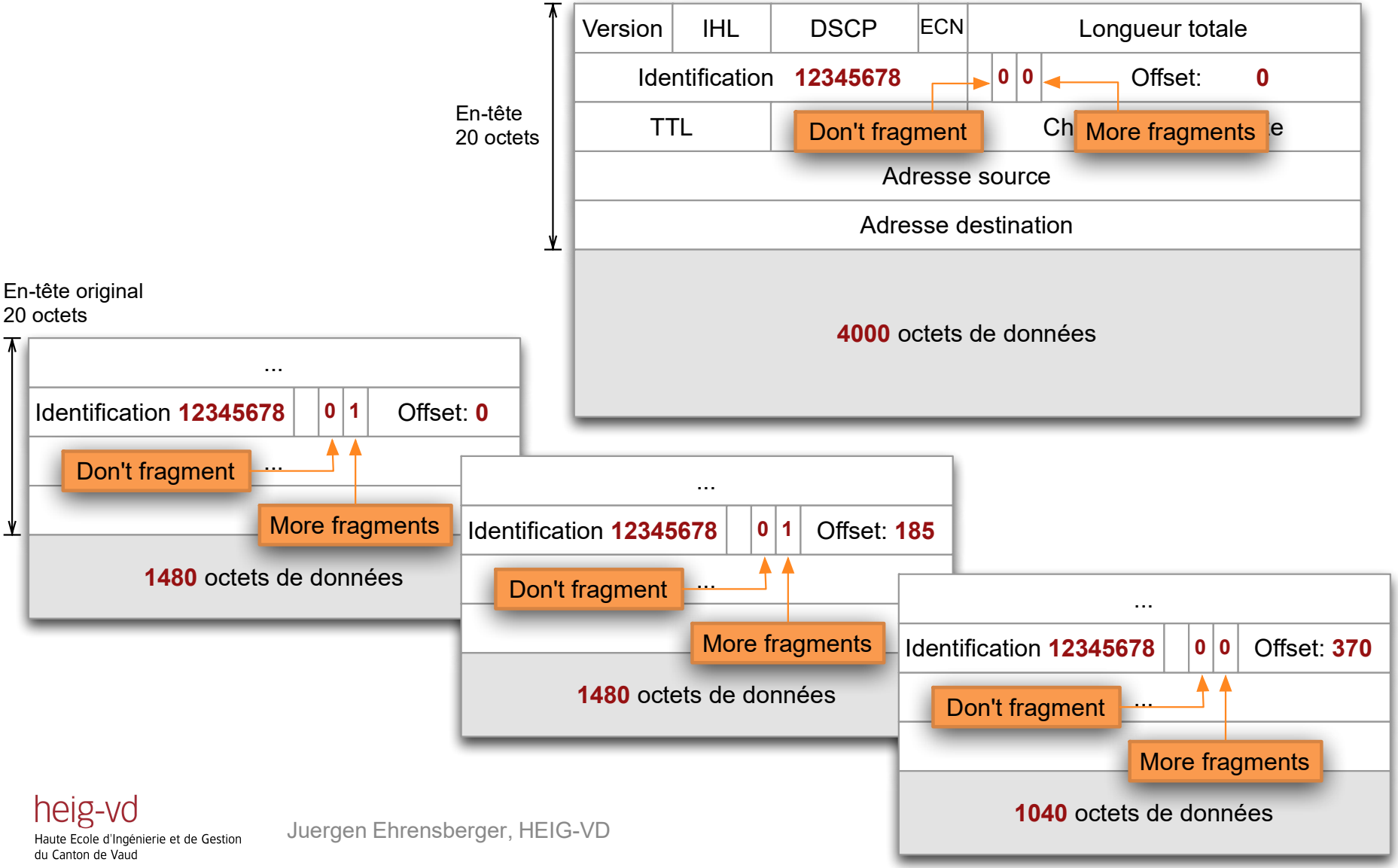
- Un routeur (ou la source) fragmente un datagramme s'il est trop long pour l'interface
  - Ethernet: 1500 octets
  - WLAN: 7981 octets
- Chaque fragment est un datagramme complet
  - Les fragments sont acheminés de manière indépendante
  - Ils peuvent être encore fragmentés plus loin
- Le destinataire 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



Fragmentation



Adressage IP (version 4)

- L'adressage IP est un élément essentiel d'Internet
- Chaque interface réseau connectée à Internet doit avoir une adresse IP pour être atteignable
  - Un PC peut avoir plusieurs adresses IP

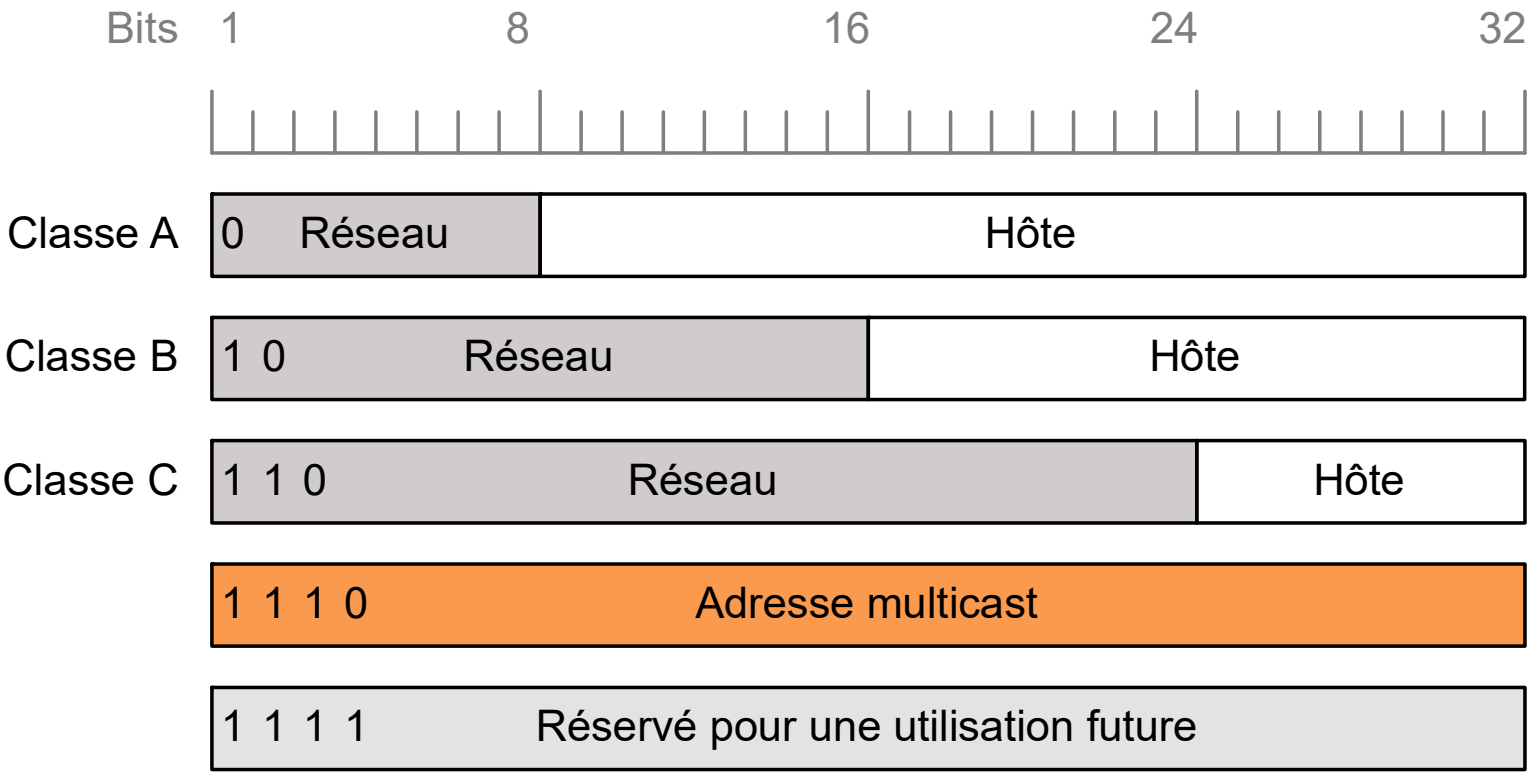
- Certaines adresses IP ont une signification particulière
  - Adresses locales
  - Adresses broadcast

Structure des adresses IPv4

- Longueur: 4 octets
  - Notation décimale pointée: 193.10.4.3
- Contient deux parties
  - Identificateur de réseau (Network ID)
    - Assigné par une autorité (par exemple ISP)
  - Identificateur de machine (Host ID)
    - Assigné par l'entreprise, l'organisation ou l'utilisateur

Classes d'adresses

- Selon la longueur du préfixe réseau, on distingue plusieurs classes d'adresses



Classes d'adresses

Classe	Préfixe réseau	Suffixe machine	Plage d'adresses	Exemple	Commentaire
A	8 bits	24 bits	1.0.0.0 – 127.255.255.255	85.218.0.70	126 réseaux, 16 Mio hôtes
B	16 bits	16 bits	128.0.0.0 – 191.255.255.255	128.178.50.12	16k réseaux, 64k hôtes
C	24 bits	8 bits	192.0.0.0 – 223.255.255.255	193.134.220.23	2 Mio réseaux, 254 hôtes
D			224.0.0.0 – 239.255.255.255	224.0.0.2	Adresses multicast, par exemple « Tous les routeurs »

Adresses particulières

Type	Adresses	Commentaire
Loopback	**127.x.y.z** Typiquement : **127.0.0.1**	Typiquement 127.0.0.1. Utilisé pour des tests et pour la communication entre processus de la même machine.
Broadcast local	**255.255.255.255**	Broadcast à l'intérieur d'un réseau
Adresse du réseau	Préfixe réseau + tous les autres bits à 0 Exemple: **132.2.0.0**	Première adresse du réseau. Ne peut pas être assignée à une machine.
Adresse broadcast d'un réseau	Préfixe réseau + tous les autres bits à 1 Exemple: **132.2.255.255**	Dernière adresse du réseau. Broadcast depuis l'extérieur. Ne peut pas être assignée à une machine.

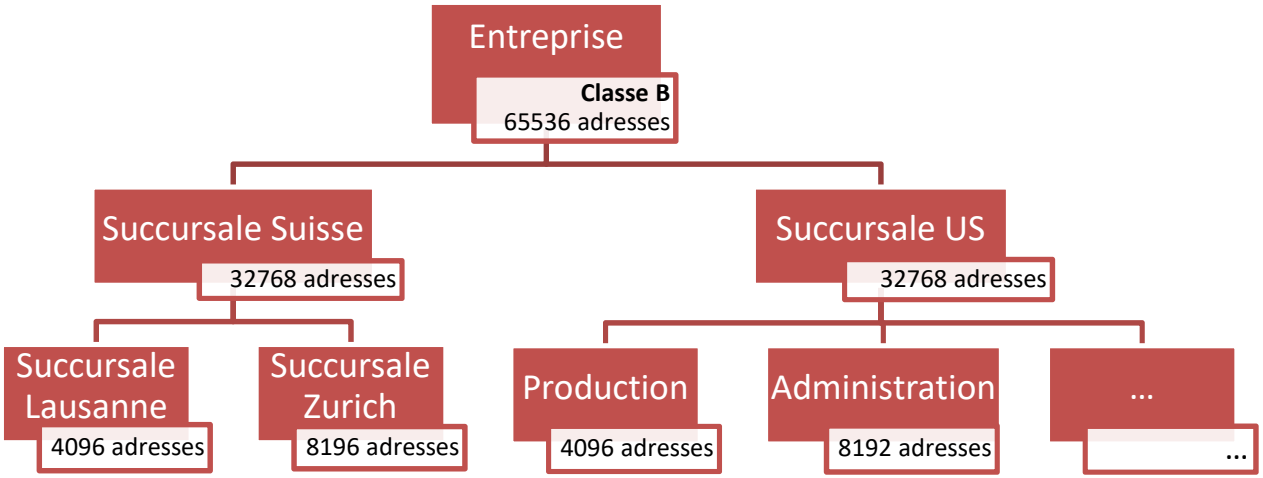
Sous-réseaux et adressage sans classes

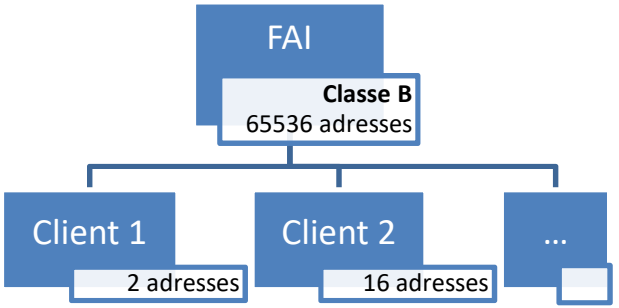
- Les classes fixes d'adresses ont plusieurs inconvénients
  - Une entreprise avec 257 machines aurait besoin d'un réseau classe B
    ➔ Gaspillage d'adresse
  - Une PME avec 2 machines a besoin d'un réseau classe C
    ➔ Gaspillage d'adresses
  - Une entreprise avec un réseau classe B ou ne peut pas subdiviser la plage d'adresse et de les gérer par département
    ➔ Gestion difficile

- Les sous-réseaux permettent de résoudre ces problèmes

Sous-réseaux

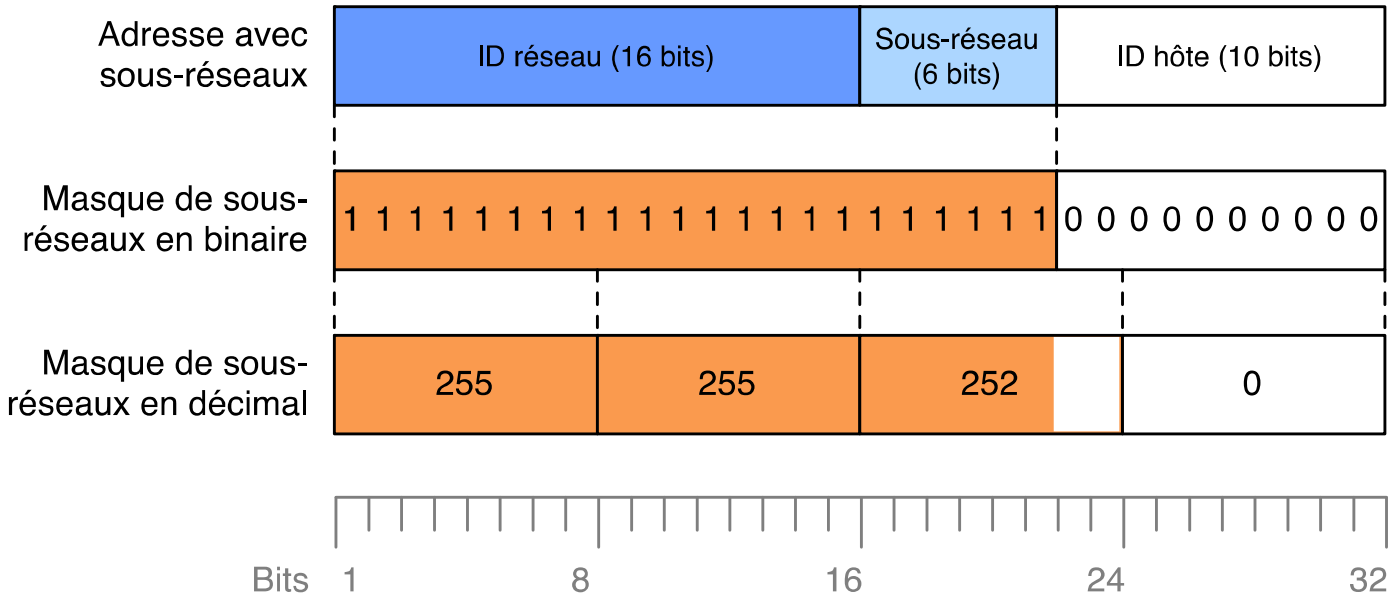
- Idée
  - Subdiviser une plage d'adresse en plages plus petites et les allouer a différents réseaux physiques





Masque de sous-réseaux

- Permet de diviser une plage d'adresses en sous-réseaux
- Adressage à trois niveaux
  - Exemple: réseaux classe B



- Subdivision du réseau classe B en 2^6 = 64 sous-réseaux, chacun avec 2^{10} = 1024 stations

Calculs avec masques de sous-réseaux

Deux types de calculs

1. Déterminer un masque de sous-réseaux:

   « Une entreprise veut créer **n** sous-réseaux, avec au minimum **x** machines par sous-réseau. Quel masque choisir ? »

1. Déterminer les adresses d'un sous-réseau:

   « Votre adresse IP est **x**. Votre masque est **m**. Quelles sont les adresses IP qui font partie de votre sous-réseau ? »

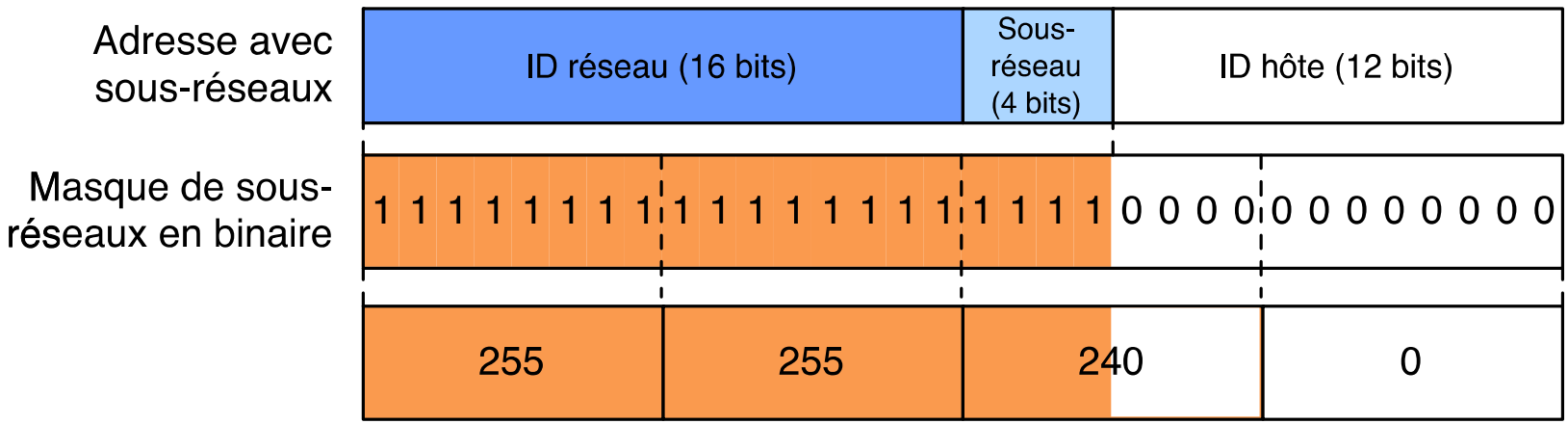
Exemple: déterminer un masque de sous-réseaux

Données

- Réseau classe B
- Au minimum 10 sous-réseaux
- Au minimum 600 machines par sous-réseau

Calcul

- Classe B ➔ 16 bits réseau, 16 bits disponibles pour sous-réseaux + ID hôte
- 10 sous-réseaux ➔ 4 bits permettent 2^4 = 16 sous-réseaux
- 600 machines ➔ 10 bits permettent 2^{10} = 1024 machines par sous-réseau
- Deux bits restent, à ajouter aux sous-réseaux ou aux machines par sous-réseau

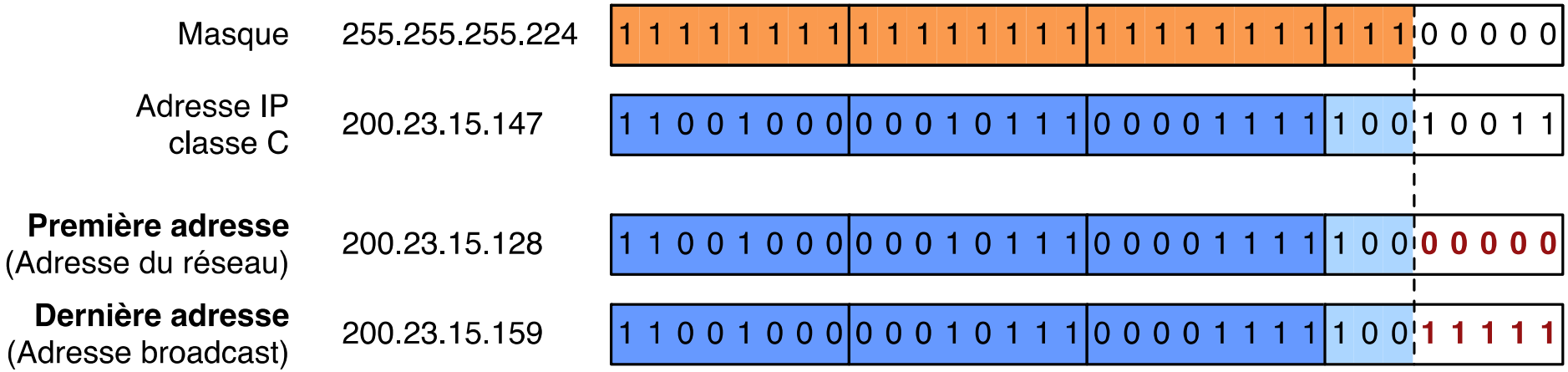


Exemple: déterminer les adresses d'un sous-réseau

Données

- Votre adresse est 200.23.15.147
- Votre masque de sous-réseau est 255.255.255.224

Calcul



Utilisation des addresses d'un sous-réseau

- La première adresse d'une plage est l'adresse du sous-réseau
- La dernière adresse d'une plage est l'adresse de broadcast / diffusion dirigée du sous-réseaux
  - Signifie : toutes les machines du sous-réseau
- Les deux adresses ne peuvent pas être assignées à des machines

- Exemple:
  - Sous-réseau avec 4 bits / 16 adresses
  - 14 adresses utilisables

Notation CIDR

- CIDR: *Classless Interdomain Routing*
  - Permet de réduire la taille des tables de routage en fusionnant des réseaux pour créer des super-réseaux
- CIDR introduit une nouvelle notation
  - Exemple: 200.123.230.13**/21**
    - Indique masque avec les premiers 21 bits à 1
    - Correspond à un masque de 255.255.248.0

Exercices

- Vous disposez de l'adresse réseau classe B 168.27.0.0. Proposez un masque de sous-réseaux qui vous permet de définir au moins 14 sous-réseaux disposant chacun d'au moins 2000 adresses hosts.

- Supposez que l'adresse IP d'une interface est 128.12.34.71 et le masque de sous-réseau 255.255.240.0. Trouvez les valeurs suivantes :
  - ID de sous-réseau,
  - ID d'hôte,
  - Adresse de diffusion dirigée.

Adressage privé

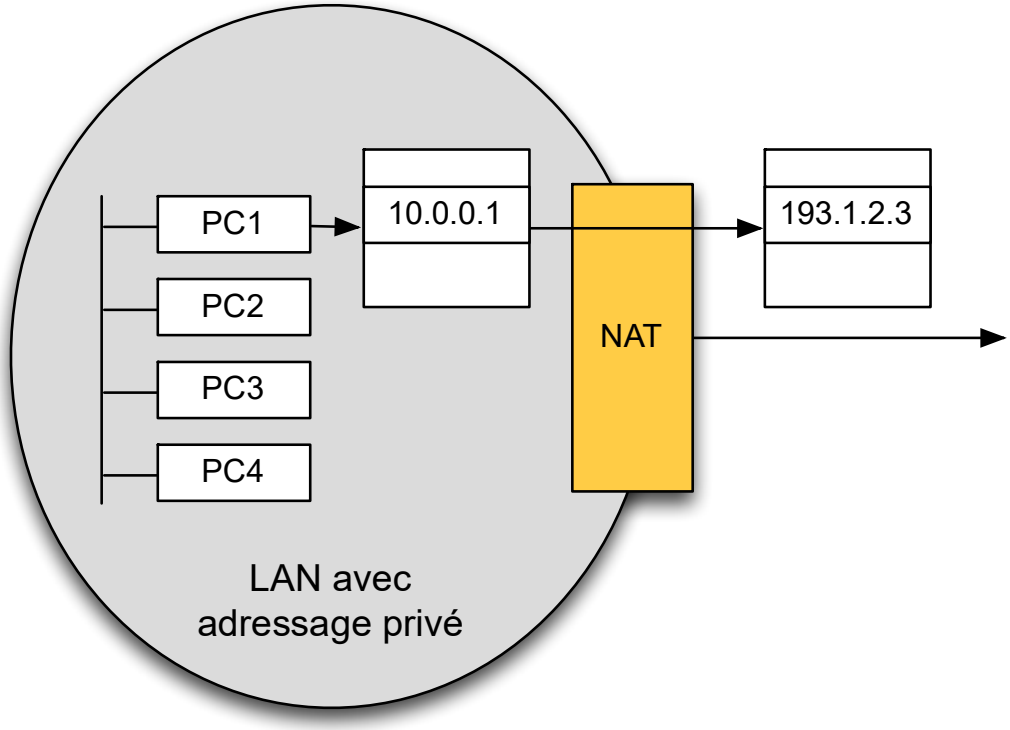
- Problème: manque d'adresses IPv4
- Idée: Réutilisation d'adresses IP
  - Une organisation utilise des adresses privées à l'intérieur du réseau
  - Pour la communication avec l'extérieur, une adresse publique est assignée de manière temporaire

Adresses privées

Adresses			Commentaire
10.0.0.0	–	10.255.255.255	1 réseau classe A
172.16.0.0	–	172.31.255.255	16 réseaux classe B
192.168.0.0	–	192.168.255.255	256 réseaux classe C

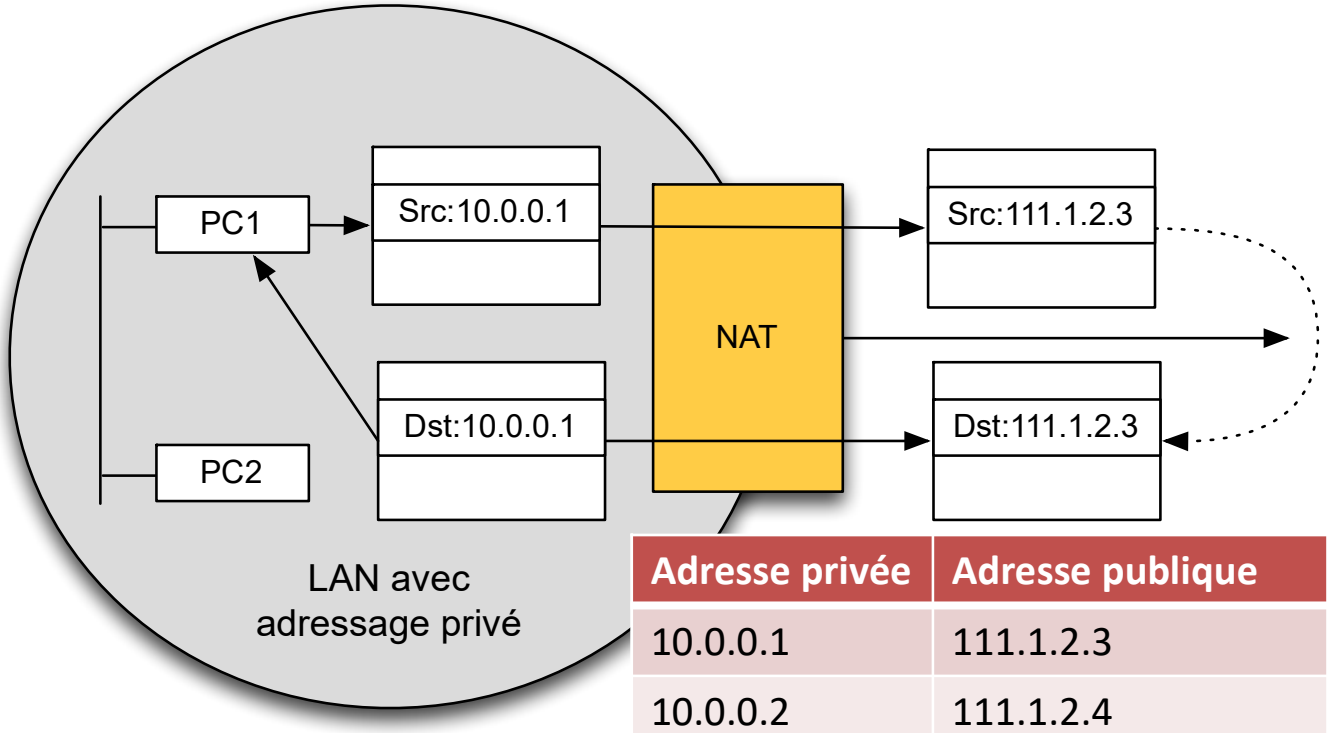
Traduction d'adresses privées

- Les adresses privées ne sont uniques et ne sont donc pas utilisables sur Internet
  - Adresses dites « non routables »
- NAT: *Network Address Translation*
  - Permet de traduire les adresses privées entre le réseau interne et Internet public



Types de NAT

- **NAT dynamique (NAT simple)**
  - L'équipement NAT dispose d'un pool d'adresses publiques
  - Les adresses publiques sont allouées temporairement à une machine dès qu'elle établit une connexion avec l'extérieur
  - Le nombre de connexions simultanées est limité par le nombre d'adresses publiques disponibles

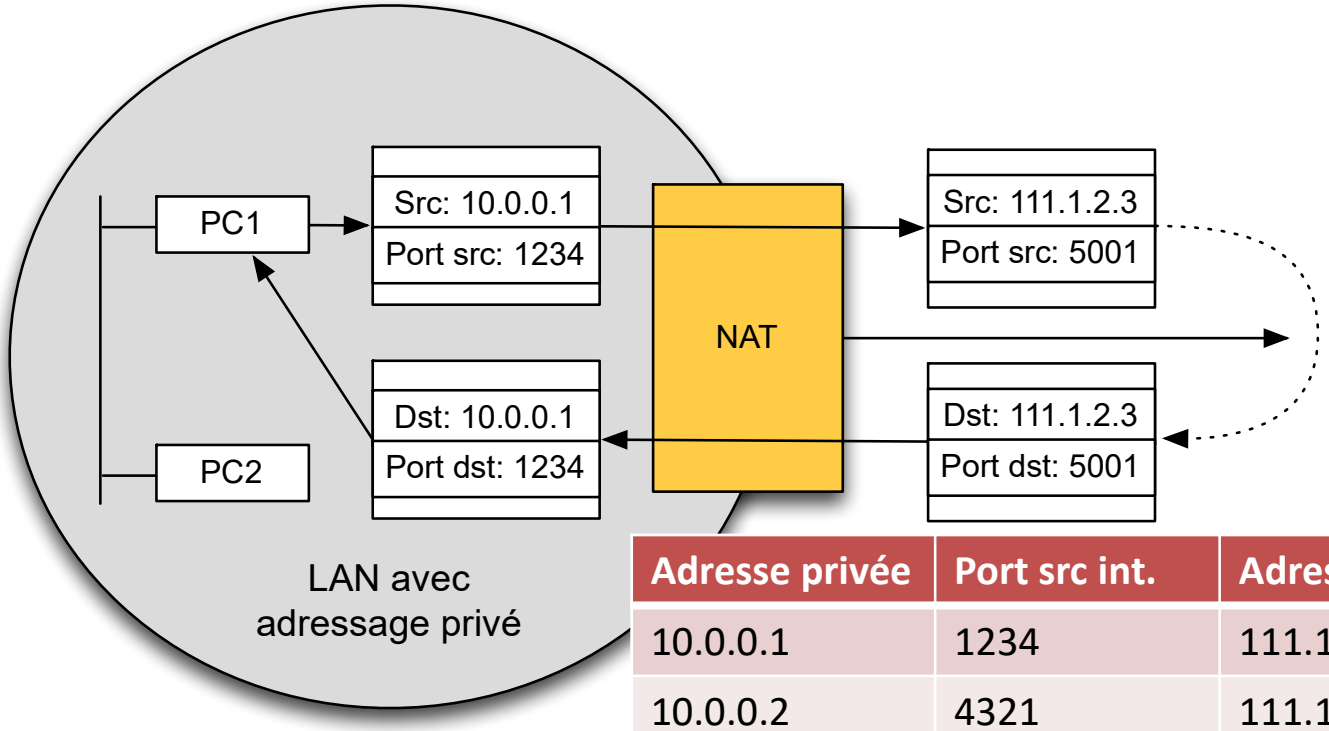


Adresse privée	Adresse publique
10.0.0.1	111.1.2.3
10.0.0.2	111.1.2.4

Table de traduction du NAT

Types de NAT

- **NAPT (*Network Address Port Translation*)**
  - Une seule adresse publique est partagée entre plusieurs connexions simultanées
  - L'équipement NAT modifie l'adresse source privée ainsi que le port TCP/UDP source du paquet sortant
  - Grâce au port source, le NAT peut distinguer les différentes connexions



Adresse privée	Port src int.	Adresse publique	Port src ext.
10.0.0.1	1234	111.1.2.3	5001
10.0.0.2	4321	111.1.2.3	5002

Types de NAT

- Beaucoup d'autres variantes de NAT existent
  - Source NAT et Destination NAT
  - NAT statique
  - NAT symétrique, NAT full-cone, …
  - IP masquerading
  - et beaucoup d'autres…