Architecture et langages Web
(NFA040)

Protocole TCP/IP[1]

Tristan Crolard

Laboratoire CEDRIC
Equipe « Systèmes Sûrs »

tristan.crolard@cnam.fr

cedric.cnam.fr/sys/crolard

1. Cours basé sur les supports de Sami Taktak

Bibliographie

[Lohier 04]. « Internet, services et réseaux »,
Stéphane Lohier, Dominique Présent. Dunod, 2004

[Moreno 03]. « Unix administration : Systèmes et réseaux »,
Jean-Michel Moreno. Dunod, 2003.

[Pujolle 01]. « Initiation aux réseaux »
Guy Pujolle. Eyrolles, 2001.

[Pujolle 08]. « Les réseaux »
Guy Pujolle. Eyrolles, 2008.

[Servin 03]. « Réseaux et télécoms »
Claude Servin. Dunod, 2003.

[Tanenbaum 11]. « Réseaux »,
Andrew S. Tanenbaum, David J. Wetherall. Pearson, 2011

Les figures de ces supports de cours sont tirées de ces ouvrages.

Protocole Réseau

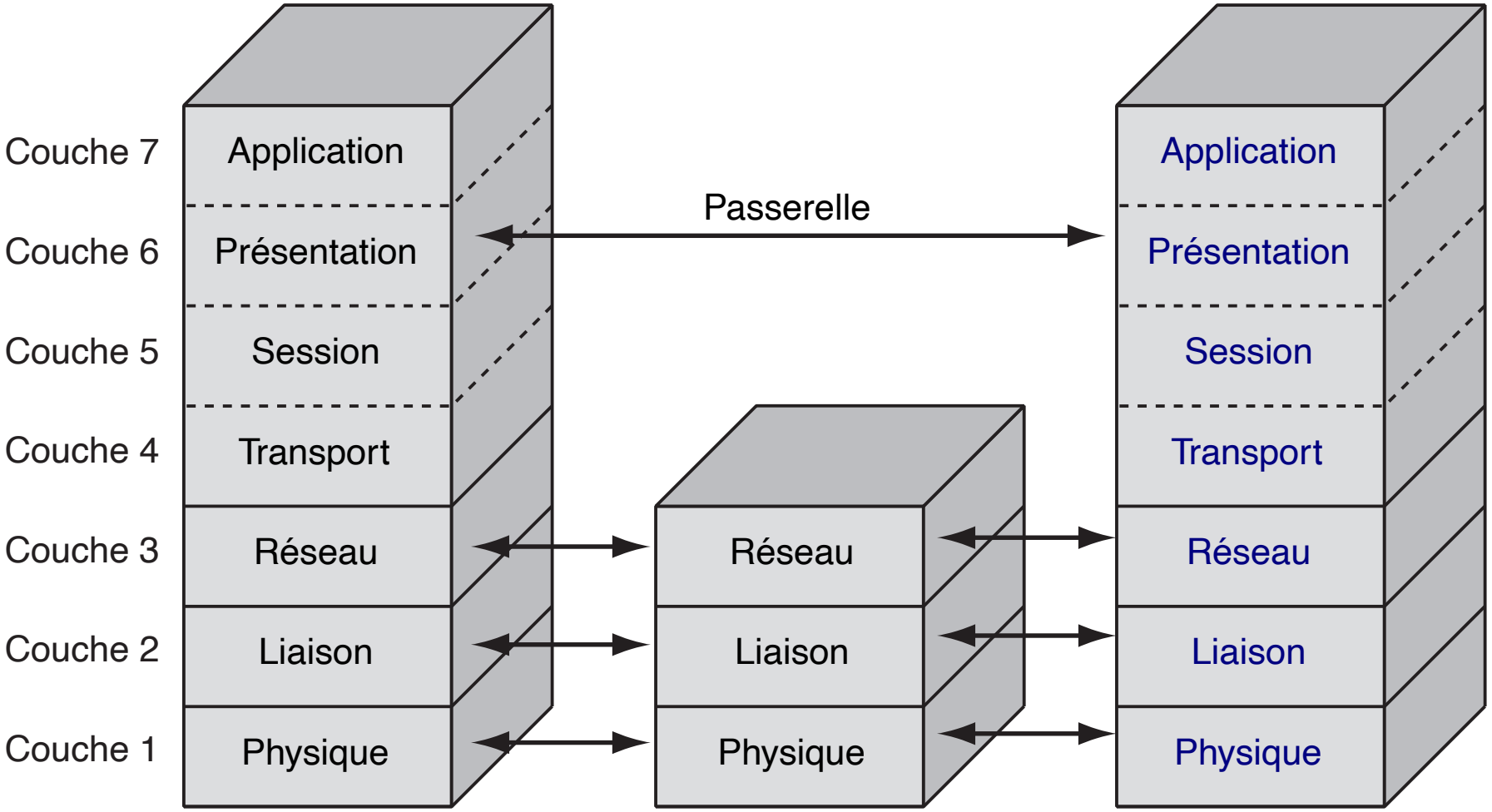
Définition. (Protocole Réseau) *Un protocole définit un ensemble de règles suivies par les équipements dans le but d'échanger des informations. Les formats des informations font partie intégrante du protocole.*

- Liés aux services : HTTP pour le Web, SMTP, POP et IMAP pour l'e-mail, ...
- Liés à l'acheminement des données : TCP pour le transport, IP pour l'adressage, RIP pour le routage, ...
- Liés à l'établissement d'une liaison : PPP pour une liaison entre un usager et un FAI, ATM pour les liaisons d'infrastructure, ...

Modèle TCP/IP

- Initialement conçu pour ARPANET
- Définit l'architecture des réseaux de l'Internet
- Normalisé par l'IETF
- TCP/IP:
  - TCP: Transport Control Protocol
  - IP: Internet Protocol
- Constitué de 4 couches

Modèles OSI et TCP/IP



Terminologie TCP/IP

Dénomination des unités de données:

- Bit au niveau physique
- Trame au niveau liaison (ethernet, WiFi, ...)
- Paquet ou datagramme au niveau réseau (IP)
- Segment au niveau transport (TCP)
- Information/données au niveau application

Couche Lisaison

- N'est pas normalisée par IETF
- Normalisée par d'autres organismes: IEEE, ISO, UIT, ...
- Réseaux locaux:
  - Ethernet (IEEE 802.3)
  - WiFi (IEEE 802.11)
- Réseaux d'opérateurs:
  - X25 (UIT)
  - ATM (UIT)

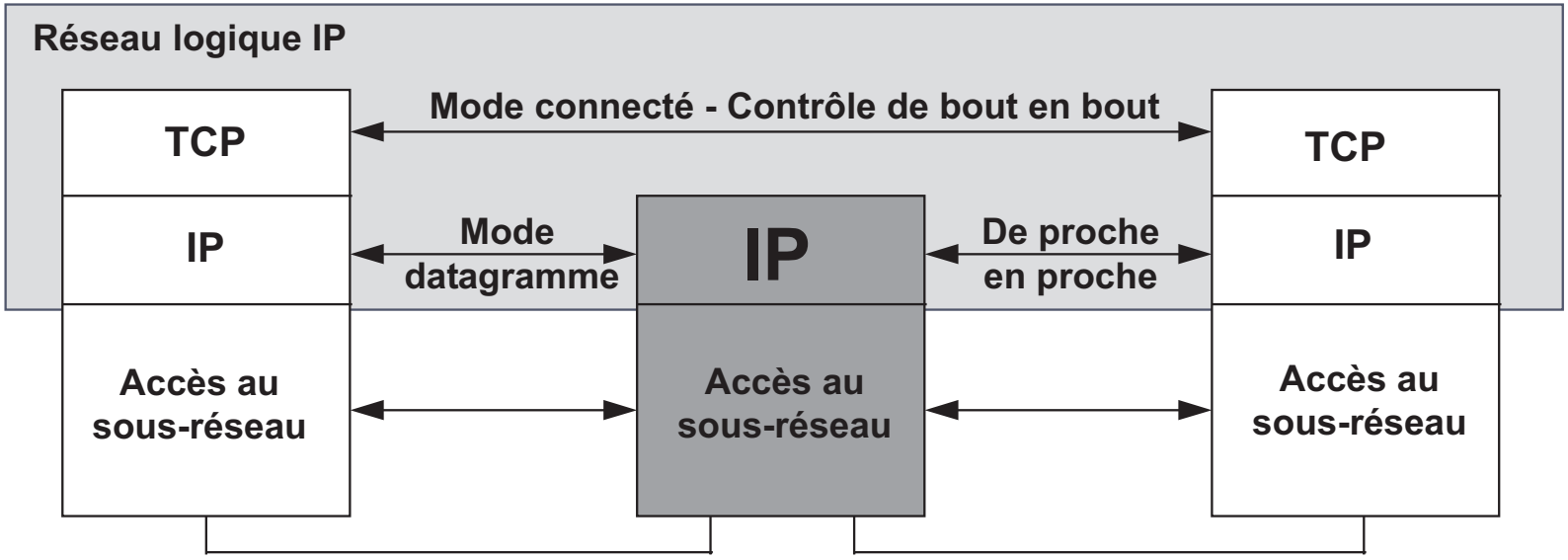
Modèle TCP/IP

- Protocole IP :
  - En charge de l'adressage et du routage des paquets
  - Fonctionne en mode non connecté et non fiable
- Protocole TCP :
  - Mode connecté et fiable
  - Retransmission de paquets en cas de perte
  - Garantit la réception des paquets dans l'ordre
  - Contrôle de flux
  - Contrôle de congestion
- Protocole UDP (User Datagram Protocol) :
  - Mode non connecté
  - Non fiable

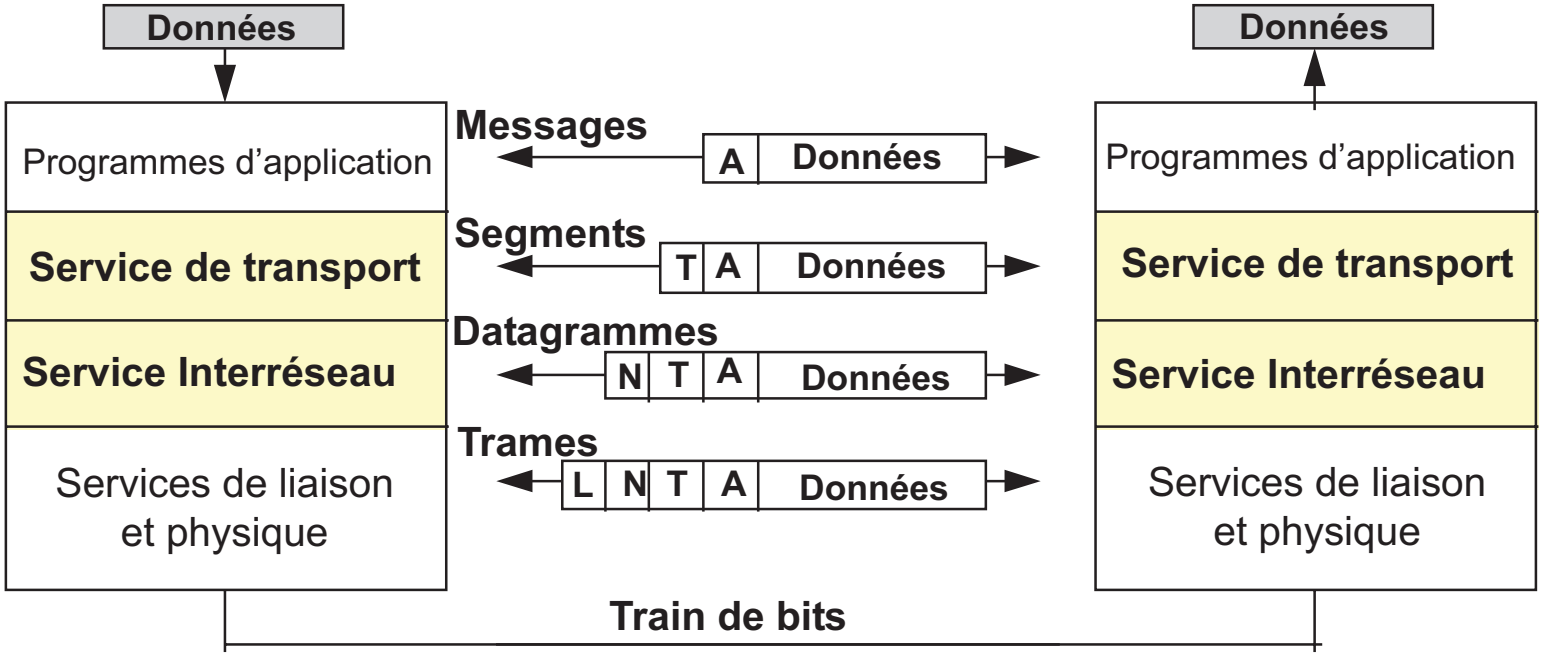
Modèle TCP/IP
TCP vs UDP

- Protocole TCP :
  - Adapté aux applications n'ayant pas de contrainte de temps mais exigeant des données intègres
  - Exemple :
    - Protocole de transfert de fichiers, FTP
    - Protocole de messagerie, SMTP, POP, IMAP
    - Consultation de page web, HTTP
- Protocole UDP :
  - Adapté aux applications « temps réel »
    - Téléphonie sur IP
    - Vidéo-conférences
    - Service de noms, DNS

Modèle TCP/IP
couche transport



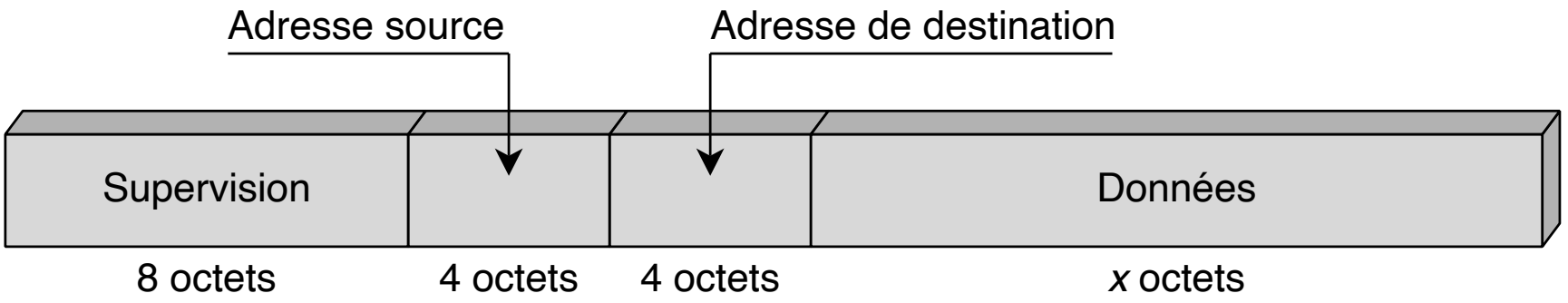
Modèle TCP/IP
Encapsulation



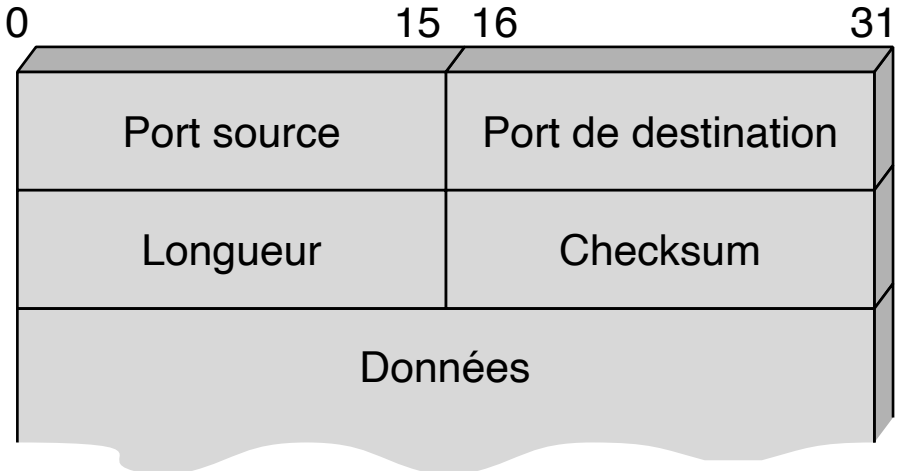
Principe d'Encapsulation

- Réception par le client
- Traité en premier par la couche Ethernet : contrôle de l'adresse physique et vérification de l'intégrité
- Désencapsulation des données et passage à la couche supérieure IP, puis TCP
- Principale inconvénient de l'encapsulation :
  - Gaspillage de bande passante induit par l'ajout d'entêtes
  - Latence dße au passage à travers les différentes couches

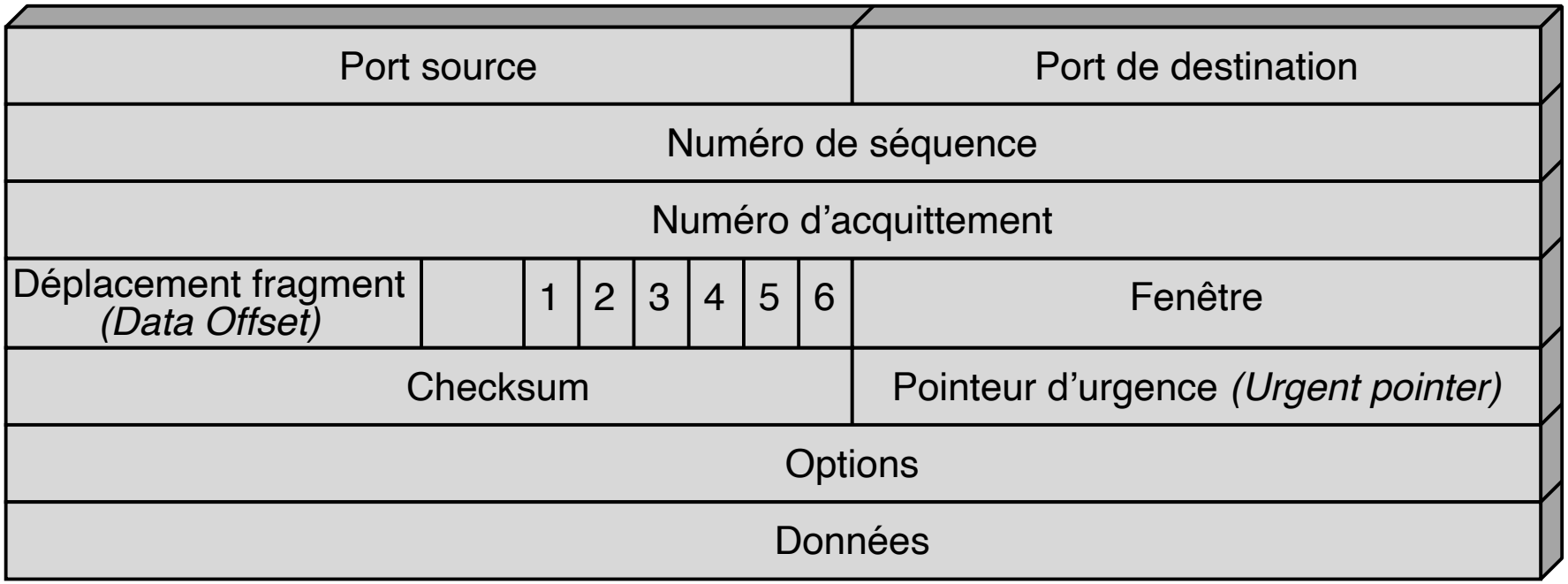
Entête IP v4


Adresse source
Adresse de destination
Supervision
Données
8 octets
4 octets
4 octets
x octets

Segment UDP


0
15
16
31
Port source
Port de destination
Longueur
Checksum
Données

Segment TCP


Port source
Port de destination
Numéro de séquence
Numéro d'acquittement
Déplacement fragment
(Data Offset)
1
2
3
4
5
6
Fenêtre
Checksum
Pointeur d'urgence (Urgent pointer)
Options
Données

Rôle de la Couche Internet
Protocole IP

- Fournir une méthode d'adressage unique et universelle des machines sur Internet : l'adresse IP
- Assurer une fonction de routage des paquets sur le réseau à partir de l'adresse IP
- Assurer l'interface entre les couches hautes et basses, notamment par la fragmentation et le réassemblage des données

Protocole IP

- IP (Internet Protocol): initialement décrit dans la RCF 791 en 1981
- 2 versions du protocole cohabite sur Internet: IPv4 et IPv6
- Protocole exécuté sur les hôtes et les routeurs
- Protocole sans connexion
- Non fiable (pas d'acquittement), pas de contrôle de flux, pas de contrôle de congestion
- Prend en charge le routage, l'adressage, la fragmentation et le réassemblage des paquets IP appelés datagrammes IP

Structure des Adresses IPv4

- Adresse codée sur 4 octets (32 bits)
- Écrite en notation décimale pointée: valeur décimale de chaque octet séparée par un point (192.168.0.1)
- Adresse découpée en 2 parties:
  - Première partie identifiant le réseau, généralement appelée « préfixe réseau »; notée Net-id dans la suite
  - Deuxième partie identifiant l'équipement dans le réseau; notée Host-id dans la suite
- Soit N le nombre de bits alloués au Net-id et H le nombre de bits alloués au Host-id:
  - Nombre de réseaux différents pouvant être créés: 2^N
  - Nombre d'adresses disponibles pour les équipements: $2^H - 2$

Adresses Particulières

- Notation CIDR (Classless Inter Domain Routing)
- `0.0.0.0`: adresse utilisée pour indiquer n'importe quelle adresse
- `Net-id`, `Host-id=0`: adresse du réseau (`Host-id` = 0), ex. `192.168.0.0/24`
- `Net-id`, `Host-id` avec tous les bits à 1: adresse de diffusion dans le réseau Net-id, ex. `192.168.255.255`
- `255.255.255.255`: broadcast local (non relayé par les routeurs)
- `Net-id=127`, `Host-id` $\neq 0$: adresse locale (localhost)
- Adresses de réseaux privés :

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	$2^{32-8} = 16\ 777\ 216$
172.16.0.0/12	172.16.0.0 – 172.31.255.255	$2^{32-12} = 1\ 048\ 576$
192.168.0.0/16	192.168.0.0 – 192.168.255.255	$2^{32-16} = 65\ 536$

Masque de Réseau

Grandeur associée à un réseau et qui a le format suivant:

- Tous les bits `Net-id` valent 1
- Tous les bits de `Host-id` valent 0
- Utilisé par les routeurs pour identifier le réseau de destination d'un paquet
- `ET` logique réalisé bit à bit entre une adresse IP et un masque de réseau: fournit l'adresse du réseau auquel appartient la machine

Masque de Réseau

- Masque de réseau associé au réseau `193.55.44.0/24`:
  - `255.255.255.0`
- Masque de réseau associé au réseau `193.55.44.0/25`:
  - `255.255.255.128`
- Calcule du réseau de l'adresse IP : `193.55.44.12` avec masque de réseau: `255.255.255.0`
  - adresse IP en binaire:
    `1100 0001 . 0011 0111 . 0010 1100 . 0000 1100`
  - masque en binaire:
    `1111 1111 . 1111 1111 . 1111 1111 . 0000 0000`
  - ET logique entre l'adresse IP et le masque:
    `1100 0001 . 0011 0111 . 0010 1100 . 0000 0000`
  - Adresse du réseau en décimal:
    `193.55.44.0`

Limitation d'IPv4

- IPv4 définie une plage d'adressage de 4 milliards d'adresses
- Semblait largement suffisant au début d'Internet (années 1970)
- Une partie des adresses non utilisables:
  - Utilisation privée
  - Multicast (adresse entre 224.0.0.0 et 239.255.255.255)
  - Adresses réservées (entre 240.0.0.0 et 255.255.255.255)
  - Adresses particulière (adresse de réseaux, de broadcast...)
  - Mais aussi pour raison historique: mauvaise attributions des ressources (allocation de réseau de classe A)

Classes d'adresse IP

Historiquement (jusqu'aux années 1990), 3 classes d'adresses IP:

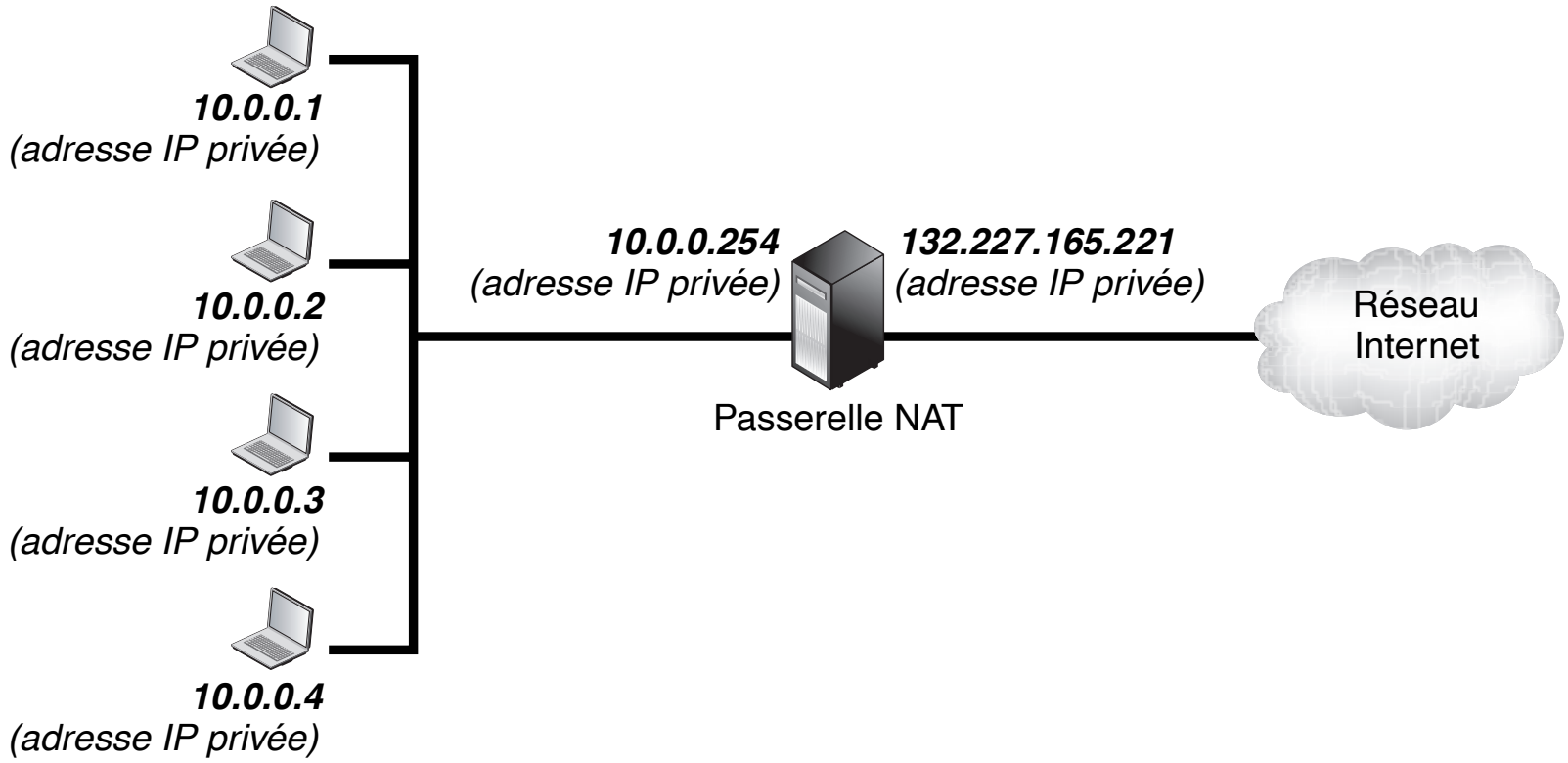
- Classe A, 1 octet pour le `Net-id`:
  - $2^{24} - 2$ adresses $\approx$ 16 millions d'adresses
  - exemple: 10.0.0.0/8
- Classe B, 2 octets pour le `Net-id`:
  - $2^{16} - 2$ adresses $= 65\,534$ adresses
  - exemple: 172.16.0.0/16
- Classe C, 3 octets pour le `Net-id`:
  - $2^{8} - 2$ adresses $= 254$ adresses
  - exemple: 192.168.1.0/24
- Réseaux de classe A entiers distribués à des entreprises et des organisations

Épuisement des Adresses IP

- 3 février 2011: annonce par l'IANA de la distribution des 5 derniers blocs d'adresses
- 15 avril 2011: annonce par l'APNIC qu'il ne dispose plus que d'1 bloc /8
- 14 septembre 2012: annonce par le RIPE NCC qu'il ne dispose plus que d'1 bloc /8
- Épuisement entre 2013 et 2015 pour les autres registres régionaux (RIR)

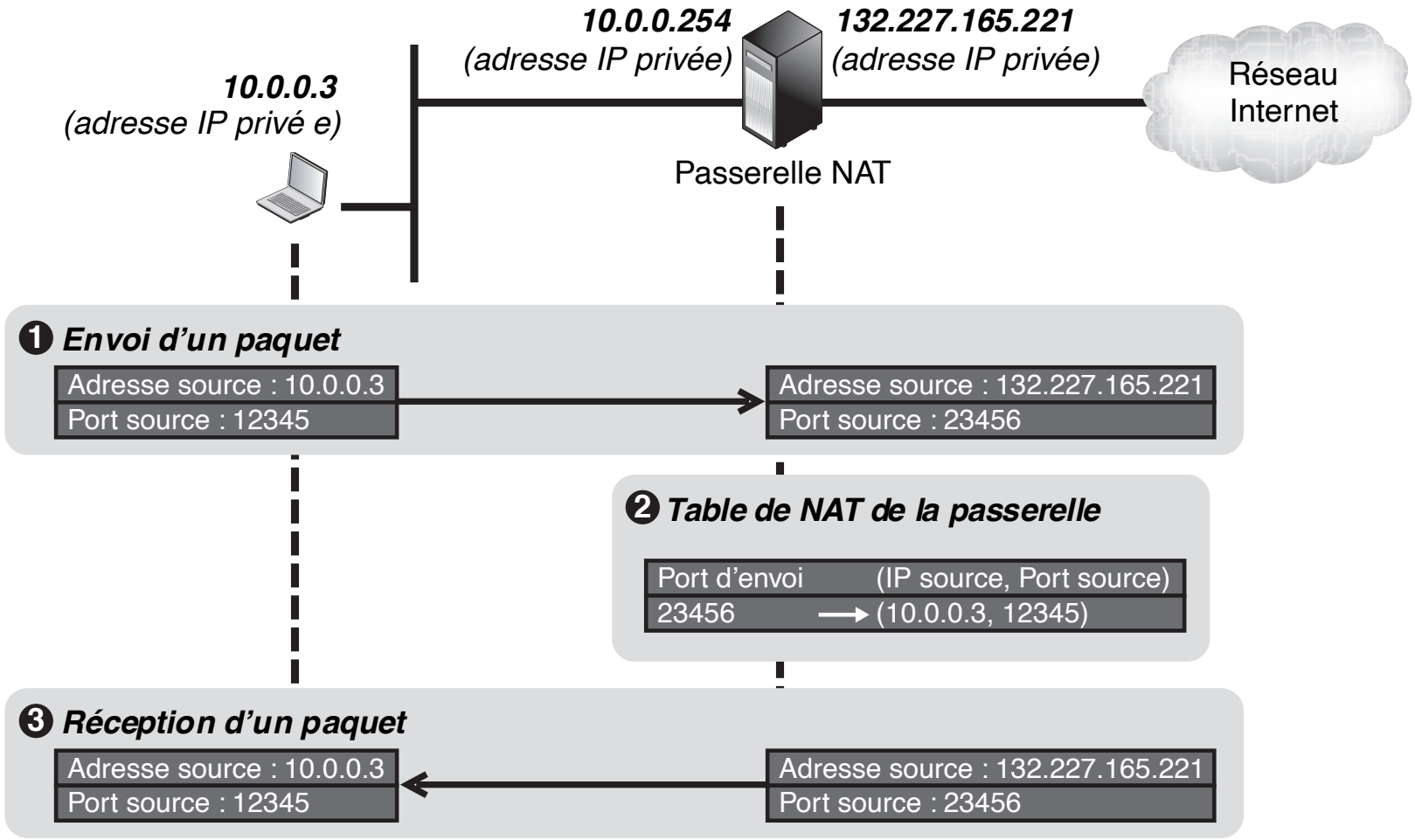
NAT (Network address translation)

- Solution partielle introduite pour protéger les réseaux locaux
- Utilisation d'adresses privées : seule l'IP du firewall est publique.



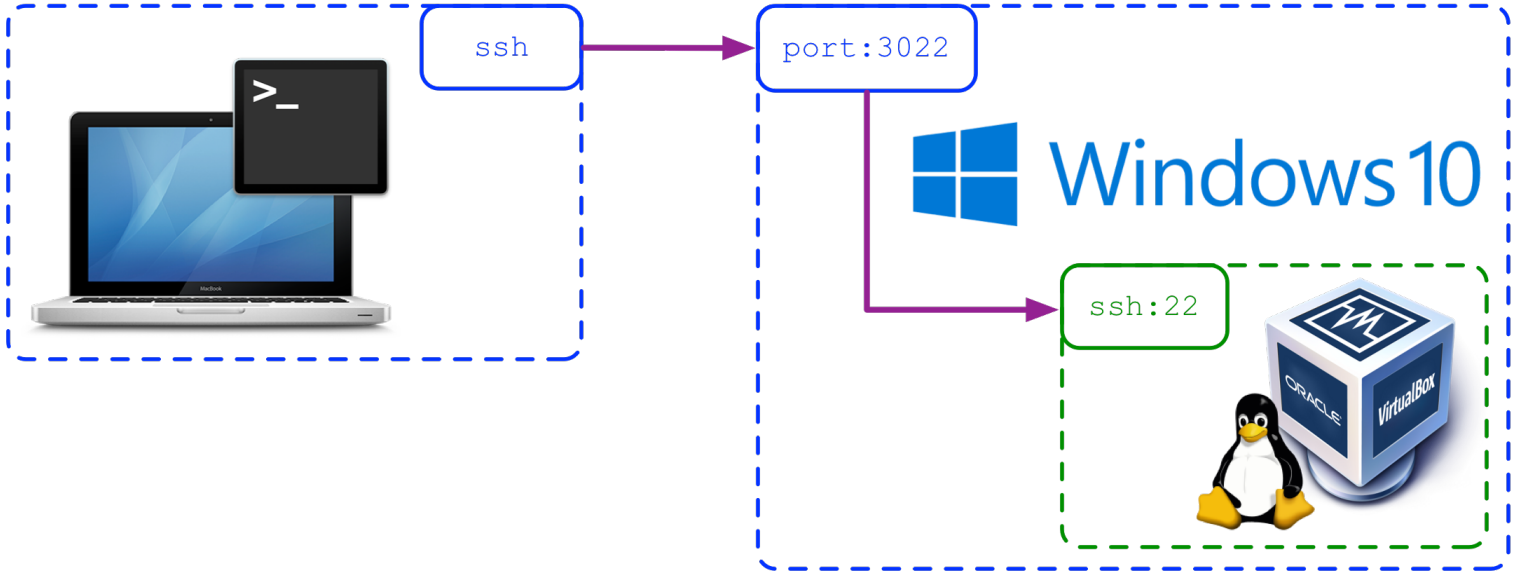
NAT : fonctionnement

- Exploite les numéros de ports pour réaliser la correspondance



NAT : redirection de port logiciel

- permet de rendre des services accessibles depuis l'extérieur
- fonctionne avec un réseau privé ou virtuel



IPv6

- IPv6 (Internet Protocol version 6): protocole réseau sans connexion de la couche 3 du modèle OSI (Open Systems Interconnection)
- Développé au cours des années 1990 sein de l'IETF
- Ses spécifications finalisées dans la RFC 2460 en décembre 1998
- Augmentation de 2^{32} à 2^{128} du nombre d'adresse
  soit 667 millions de milliards d'adresses IP par mm^2 de la surface de la Terre
- Simplification des en-têtes de paquets pour faciliter le routage
- Mécanisme de *sécurisation des communications* (IPsec)