Cours Réseaux RT 1 – R201

Promotion BUT 2024

bascou.perso.univ-pau.fr/R201

Jean-Jacques BASCOU

Plan Général du Cours R201

- Partie 1: Le Modèle TCP/IP - ARPA
  - Introduction
  - La couche Réseau (couche IP)
    - Le protocole IPv4 / Le protocole IPv6
    - Le protocole ARP (IPv4) / Le protocole ND (IPv6)
    - Le protocole ICMPv4 / Le protocole ICMPv6
  - Synthèse générale de fonctionnement
- Partie 2: Le Routage Dynamique
  - Principes du routage dynamique
  - Les algorithmes « Vecteur Distance »
  - Les algorithmes « Etats de Liens »
- Partie 3: Couche Transport UDP / TCP
  - UDP
  - TCP
- Partie 4: Les règles de filtrage
  - ACL IPv4
  - ACL IPv6

La pile « TCP/IP »

APPLICATION (~osi: application, présentation, session)
TRANSPORT (~osi: transport)
INTERNET (~osi: réseau)
ACCES RESEAU (~osi: liaison de données, physique)

La pile « TCP/IP »

NFS, SNMP	**TELNET, FTP, SMTP,...**
UDP	**TCP**
IPv4, ICMP, ARP, IPv6, ICMPv6, ND, …	
Ethernet, PPP, ATM, HDLC, …	

La Couche Réseau

- Adressage IP
- Protocole IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

Généralités

- 1 interface réseau = 1 adresse IP (au moins)

- Adresse IP (v4): 32 bits = 4 Octets
- Adresse IP (v6): 128 bits = 16 Octets

IPv4: Généralités

- Adresse IP (v4): 32 bits = 4 Octets
- Représentation décimale pointée:

11000001 00110111 11011101 00111110

⇔

193.55.221.62

IPv6: Généralités

- Adresse IP (v6): 128 bits = 16 Octets
- Représentation hexadécimale doublement pointée:

2001:0660:3102:0000:0000:0000:0001:0CDC

2001:660:3102:0000:0000:0000:1:CDC

⇔

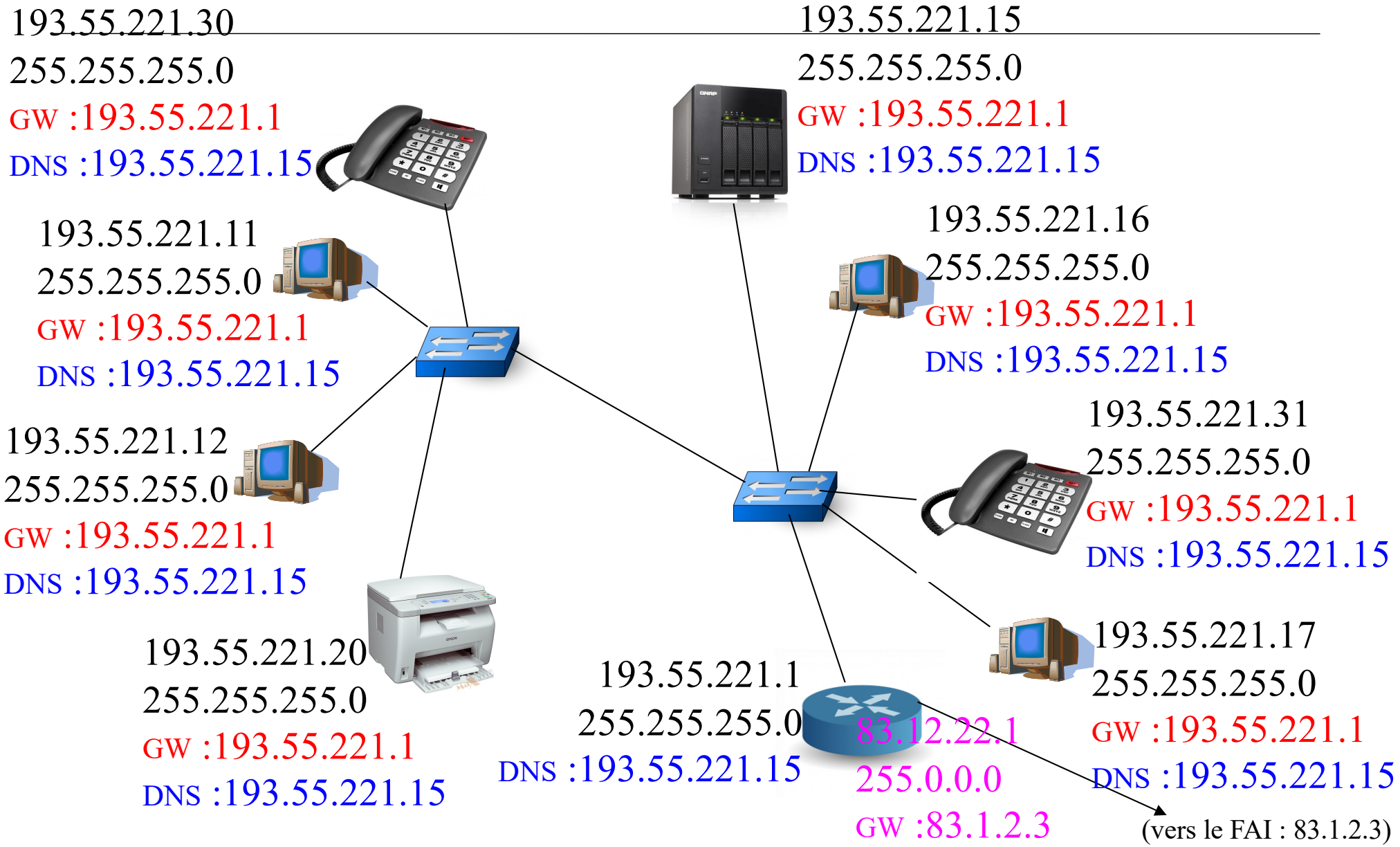
2001:660:3102::1:CDC

Adresse IPv4

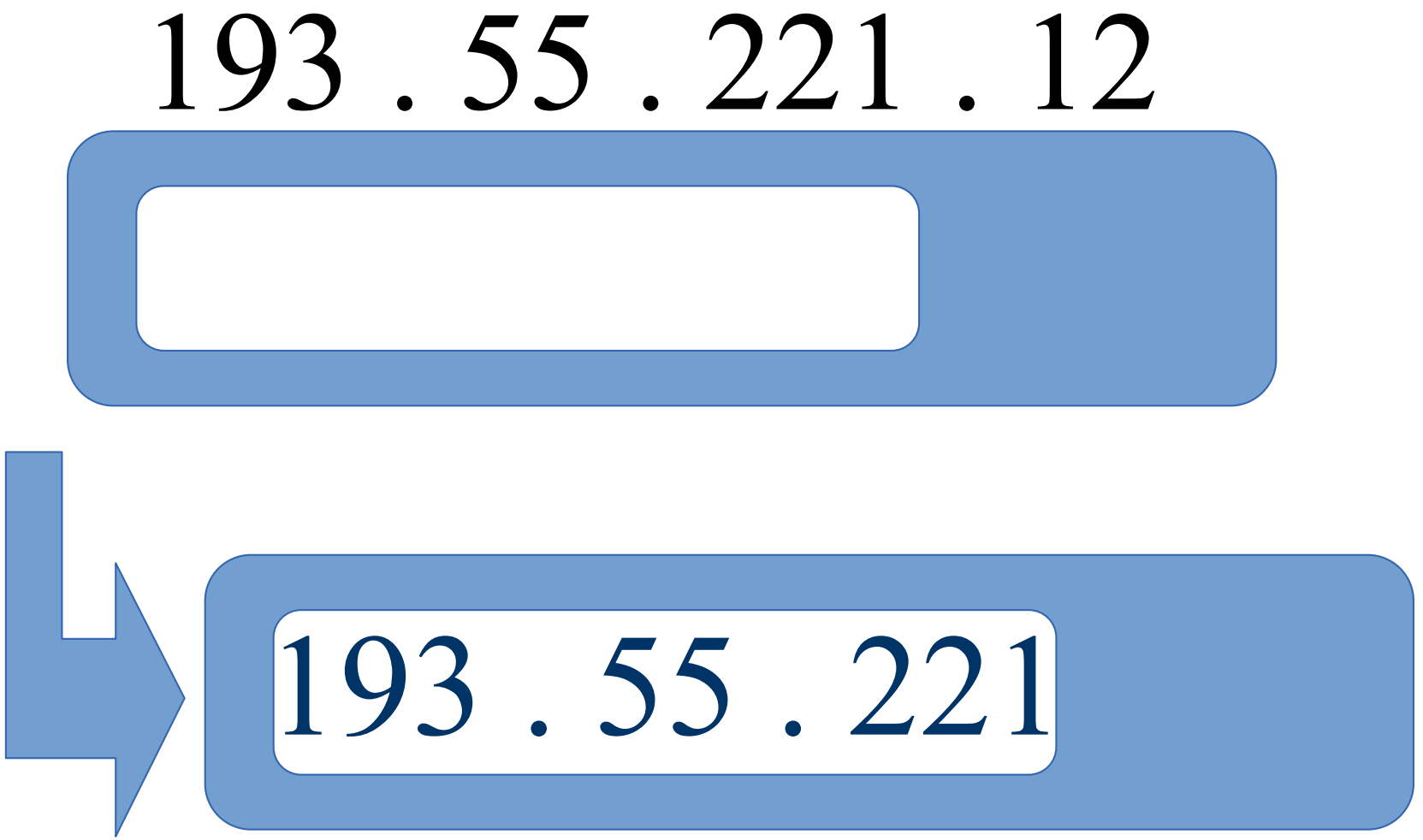
- L'adresse IP d'un équipement contient deux informations:
  - LE réseau sur lequel est connecté l'équipement
  - L'adresse de l'équipement sur le réseau

- PB: La limite entre les deux champs n'est pas fixe !!!
- ==> Comment la situer ?

Exemple de réseau d'entreprise



Masque IPv4



Masque IPv4

- La partie « ouverte » du masque
  - Correspond à des bits à 1
  - Soit 11111111 (sur un octet)
  - Soit 255 (en décimal)
- La partie « cachée » du masque
  - Correspond à des bits à 0
  - Soit 00000000 (sur un octet)
  - Soit 0 (en décimal)

Masque IPv4

- Exemple :

11000001 00110111 11011101 00111110

11111111 11111111 11111111 00000000

11000001 00110111 11011101 00000000

193.55.221.62

255.255.255.0

193.55.221.0

Masque IPv4

- Notation CIDR:
  - On compte le nombre de 1 dans le masque (les 1 sont forcément calés à gauche dans un masque)
  - Exemples:
    - 255.0.0.0 ⇔ /8
    - 255.255.0.0 ⇔ /16
    - 255.255.255.0 ⇔ /24

IPv4: adresses UNICAST

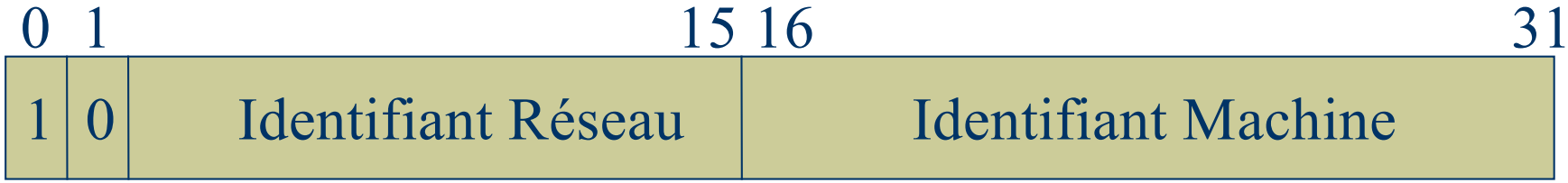
- Adresses de CLASSE A (50%):

Adresses de 0.X.X.X à 127.X.X.X

- ➔ masque: 255.0.0.0 (ou /8)
- ➔ 128 réseaux possibles
- ➔ ~ 16 777 214 éq. sur un même réseau

IPv4: adresses UNICAST

- Adresses de CLASSE B (25%):



- Adresses de 128.0.X.X à 191.255.X.X
- ➔ masque: 255.255.0.0 (ou /16)
- ➔ 16384 réseaux possibles
- ➔ ~ 65 534 équipements sur un même réseau

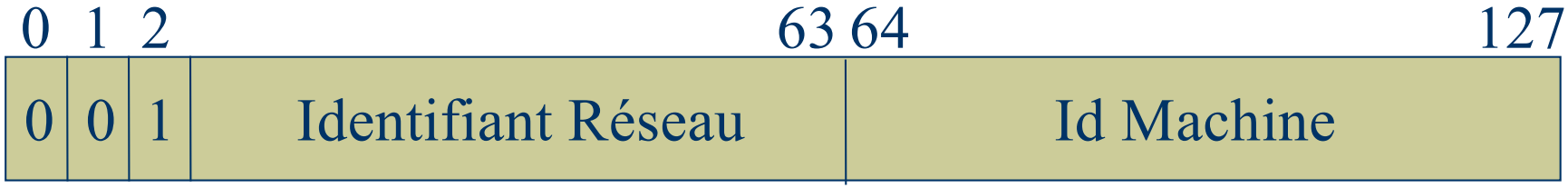
IPv4: adresses UNICAST

- Adresses de CLASSE C (12,5%):

- Adresses de 192.0.0.X à 223.255.255.X
- ➔ masque: 255.255.255.0 (ou /24)
- ➔ 2 097 152 réseaux possibles
- ➔ 254 équipements sur un même réseau

IPv6: adresses UNICAST

- Adresses:



Adresses de 2000::

à 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

- ➔ masque: /64
- ➔ 18 446 744 073 709 551 616 réseaux
- ➔ 18 446 744 073 709 551 616 équipements

Adresses Unicast

- IPv4
- 4 octets
- Notion de classes
- Masque variable
- Adresse basse réservée (rzo)
- Adresse haute réservée (broadcast)

- IPv6
- 16 octets
- Pas de classes
- Masque fixe (/64)
- Adresse basse utilisable
- Adresse haute utilisable

IPv4: adresses MULTICAST

- Adresses de CLASSE D (6,25%):

Adresses de 224.X.X.X à 239.X.X.X

- ➔ Utilisation pour multi-diffusion (multi-cast)
- ➔ Communication **unidirectionnelle**

IPv6: adresses MULTICAST

- Plusieurs niveaux de Multicast

FFxy	xx … …xx (112 bits)

- FFx1: nœud-local: les paquets ne quittent pas le nœud !
- **FFx2: link-local: les paquets ne quittent pas le segment**
- FFx5: site-local: les paquets ne quittent pas le site
- FFx8: organisation-local: les paquets ne quittent pas l'organisation … (difficile à administrer)
- FFxE: global: portée globale (idem IPv4)

(Actuellement, x=0 dans la quasi-totalité des cas)

Adresses Multicast

- IPv4
- Classe D
- Portée globale
- Utilisation exceptionnelle

- IPv6
- FFxy: ……..
- Portées différentes
- Utilisation très fréquente (surtout FF02:….)

Petite remarque …

- Adresses de CLASSE E (6,25%):

- Adresses de 240.X.X.X à 255.X.X.X
- ➔ Plage réservée pour utilisation « ultérieure »
  (c'est-à-dire définitivement perdue !)

IPv4: adresses Broadcast

- Broadcast LIMITÉ
  - 255.255.255.255
  - Adresse identique pour tous les réseaux
  - Diffusion à **tous les équipements du réseau local**
- Broadcast CIBLÉ
  - Bits de la « partie machine » à 1
  - Adresse spécifique à chaque réseau
  - Ex: 126.255.255.255 (classe A)
  - Ex: 193.55.221.255 (classe C)
  - Diffusion à **tous les équipements du réseau ciblé**

IPv6: adresses Broadcast

- Le Broadcast n'existe pas en IPv6 !
  - Trop gourmand en bande passante
  - Le Multicast remplace les utilisations du Broadcast
  - Les switch (haut de gamme) optimisent le Multicast
  - …

Adresses Broadcast

- IPv4
  - Limité
  - Ciblé
- IPv6
  - **Disparu !**
  - Adresse haute disponible pour affecter à un équipement

IPv4: adresses spéciales

- Adresse de réseau:
  - Partie machine à 0 (partie droite)
  - Exemples:
    - 193.55.221.0: adresse réseau de l'IUT (classe C)
    - 141.115.0.0: adresse réseau de l'IRIT (classe B)
    - 62.0.0.0: adresse réseau du CSC (Classe A)
      (*Computer Sciences Corporation*)
  - Attention: 141.115.0.12 est une @ d'équipement
    (l'adresse machine n'est globalement pas à « 0 »)

IPv6: adresses spéciales

- Adresse de réseau:
  - 64 bits du suffixe à 0 (partie droite)
  - **IMPORTANT**: l'adresse réseau est utilisable pour affecter à un équipement
  - Exemple:
    - 2001:660:3108:1002:: /64

IPv4: adresses spéciales

- Adresse indéfinie:
  - 0.0.0.0
  - cette @ spéciale désigne un équipement local en « recherche » d'adresse.
  - Elle est très utilisée par DHCP

IPv6: adresses spéciales

- Adresse indéfinie:
  - ::
  - cette @ spéciale désigne un équipement local en « recherche » d'adresse.
  - Elle est très utilisée par DHCPv6

IPv4: adresses spéciales

- Adresse de rebouclage:

  127.0.0.1 (localhost)

  - Désigne l'équipement local
  - Existe toujours
  - Simule un accès réseau (même sans réseau)
  - Utilisation: communications locales ou tests

IPv4: adresses spéciales

- Nouvelle adresse de rebouclage:

  127.0.1.1

  - A fait son apparition récemment
  - Utilisée sous Linux Ubunutu
  - …en fait toute la plage de classe A 127.0.0.0 peut être utilisée !

IPv6: adresses spéciales

- Adresse de rebouclage
  - ::1 (localhost)
- Utilisation:
  - Idem IPv4
  - Désigne l'équipement local
  - Existe toujours
  - Simule un accès réseau (même sans réseau)
  - Utilisation: communications locales ou tests

IPv4: adresses spéciales

- Adresses « lien local » (local link):
  - 169.254.0.0 (classe B)
- Utilisation:
  - Réseaux locaux isolés (sans serveur DHCP)
  - Permet d'utiliser le voisinage immédiat
    - Imprimantes
    - Partage de disque, …
  - Ne supporte pas le routage
- Utilisation exceptionnelle

IPv6: adresses spéciales

- Adresses « lien local » (local link):
  - FE80:: /10 (càd: FE80::, FE90::, FEA0::, FEB0::)
- Utilisation:
  - Obligatoire, sur CHAQUE interface
  - Utilisée systématiquement pour les communications locales (passerelle, …)
  - Ne supporte pas le routage
- Utilisation très fréquente !

IPv4: adresses spéciales

- Adresses non routées (non attribuées) RFC 1918:
  - classe A: 10.0.0.0 (1 adresse)
  - classe B: 172.16.0.0 - 172.31.0.0 (16 adresses)
  - classe C: 192.168.0.0 - 192.168.255.0 (256 adresses)
- Utilisation:
  - Réseaux non reliés à l'Internet (réseau privé)
  - Réseaux masqués (derrière un garde-barrière)
  - **Ces adresses ne seront jamais attribuées**

IPv6: adresses spéciales

- Adresses « site local » (local site):
  - FEC0:: /10 (**obsolètes**: ces adresses ont disparu)
- Adresses « locales uniques » (unique local):
  - FC00:: /7 (remplacent les « local site »)
  - Non officielles mais néanmoins « uniques » si demandées ici:
    - https://www.sixxs.net/tools/grh/ula/

Adresses spéciales

- IPv4
- 0.0.0.0
- @ réseau réservée
- 127.0.0.1
- 169.254.0.0
- 10.0.0.0 /8
- 172.16.0.0 /12
- 192.168.0.0 /16

- IPv6
- ::
- @ basse disponible
- ::1
- FE80:: /10
- FC00:: /7

Attribution des adresses

- L'**IANA** (Internet Assigned Numbers Authority) délègue aux autorités régionales RIR (Regional Internet Registry) des préfixes d'adresses
  - **AfriNIC** (Afrique)
  - **APNIC** (Asie/Pacifique)
  - **ARIN** (Amérique du nord)
  - **LACNIC** (Amérique latine et caraïbes)
  - **RIPE NCC** (Europe, Moyen-orient et Asie centrale)

- Les RIRs redistribuent les préfixes d'adresses aux FAI de leur région
- Les FAI distribuent les adresses à leurs clients

Limites de l'IPv4

- Pénurie d'adresses
  - Augmentation incessante du nombre d'équipements
    - Pénurie pour l'IANA: 3 février 2011
    - Pénurie pour l'AFRINIC: 15 janvier 2019
    - Pénurie pour l'APNIC: 19 avril 2011
    - Pénurie pour l'ARIN: 24 septembre 2015
    - Pénurie pour le LACNIC: 10 juin 2014
    - Pénurie pour le RIPE NCC: 14 septembre 2012

Source: http://www.potaroo.net/tools/ipv4/index.html

Limites de l'IPv4

- Contrainte géographique des adresses IPv4
  - Une adresse est liée au réseau (~ téléphone)
  - Déplacement d'équipement ➔ changement d'@IP
- Conception ancienne du protocole
  - Trop de temps de traitement sur les routeurs (TTL, CRC, en-tête variable, …)
  - Pas d'adaptation aux nouveaux services (voix, video, …)
  - Pas d'évolutivité possible

Evolutions historiques de l'IPv4

- Techniques de « subnetting » (sous réseaux)
  - Ex: Subdivision de classes A, B ou C

  ➔ limitation des pertes d'adresses
- Techniques de « supernetting » (sur réseaux)
  - Ex: Regroupement de plusieurs classes identiques

  ➔ simplification des tables de routage
- Techniques de translation d'adresses « NAT / PAT »
  - Objectif: 1 réseau = 1 adresse IP
- Nouvelle technologie: IPv6

La Couche Réseau

- Adressage IP
- Protocole IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

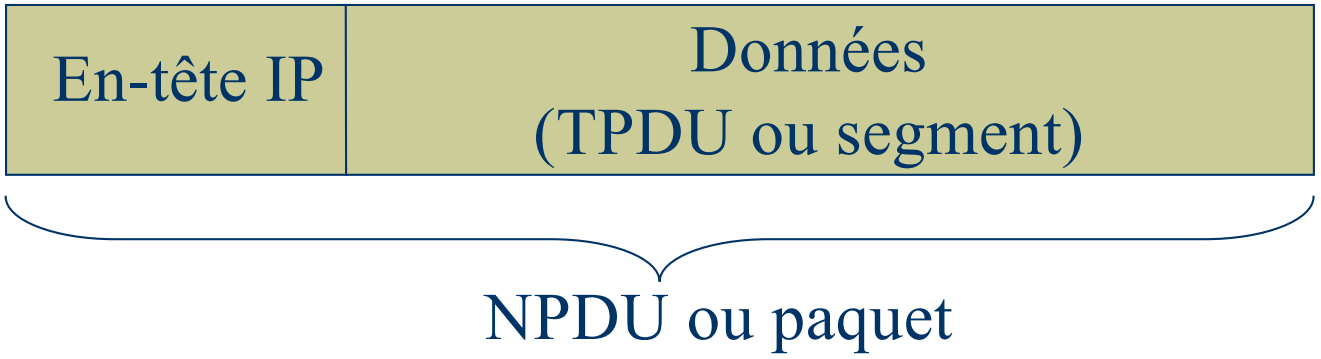
Généralités

- IPv4: RFC 791 (septembre 1981)
- IPv6: RFC 2460 (décembre 1998)

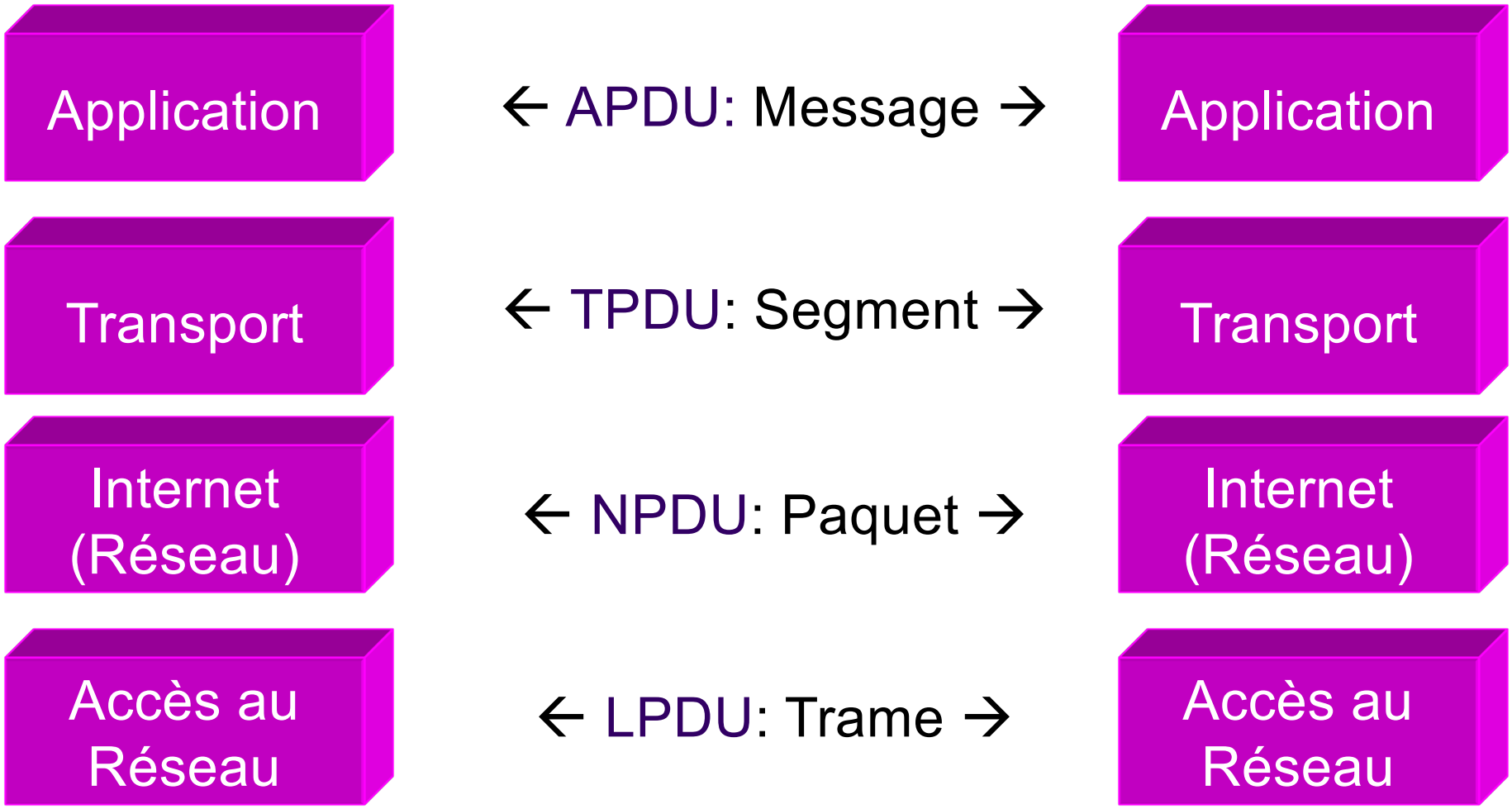
- Service en mode non connecté
  - Pas d'établissement de connexion
  - Chaque PDU (paquet) est traité indépendamment
- Service non fiable
  - Pertes, duplications, déséquencements possibles

Généralités

- PDU IP: NPDU, datagramme, paquet, …
  - 1 NPDU = En-tête IP + données (TPDU)
    - (Rappel: PDU= Protocol Data Unit)



Rappel


Application
← APDU: Message →
Application
Transport
← TPDU: Segment →
Transport
Internet (Réseau)
← NPDU: Paquet →
Internet (Réseau)
Accès au Réseau
← LPDU: Trame →
Accès au Réseau

Généralités

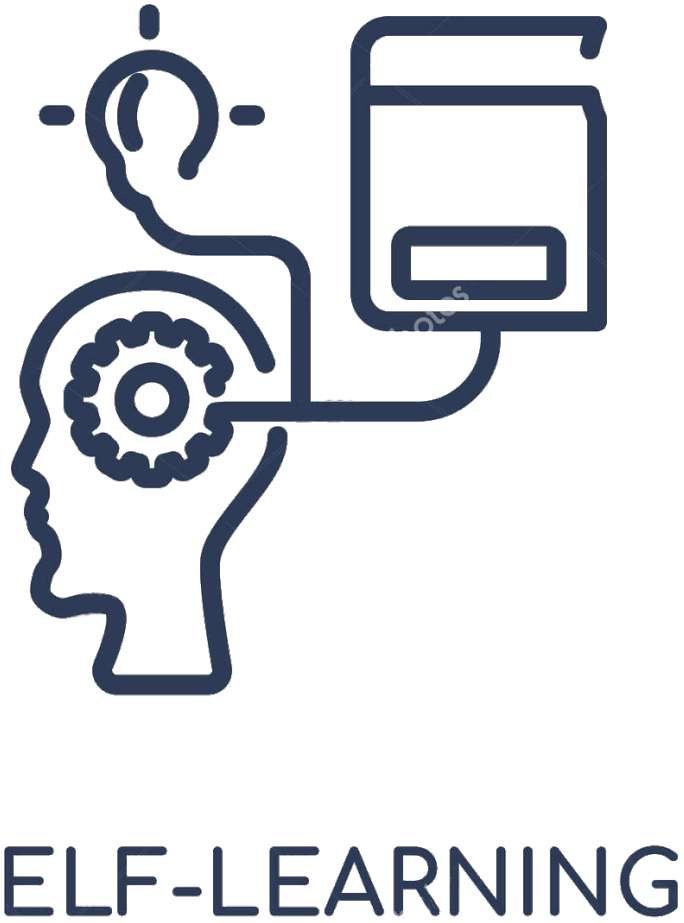
- Les **2 rôles** du protocole IP:
  - **Adaptation à la MTU** (Maximum transmission Unit)
    - Adaptation aux performances du réseau local
    - Notion de Fragmentation / Réassemblage (surtout IPv4)
    - Notion de découverte de la MTU (surtout IPv6)
  - **Routage**
    - Quel chemin à emprunter pour aller de EXP à DEST ?
    - Selon quels critères ? (rapidité, trafic, délai,… ➔ coût)

La Couche Réseau

- Adressage IP
- Protocole IP
  - Fragmentation/Réassemblage
  - Routage IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

Fragmentation / Réassemblage

- Auto-apprentissage
- Portfolio

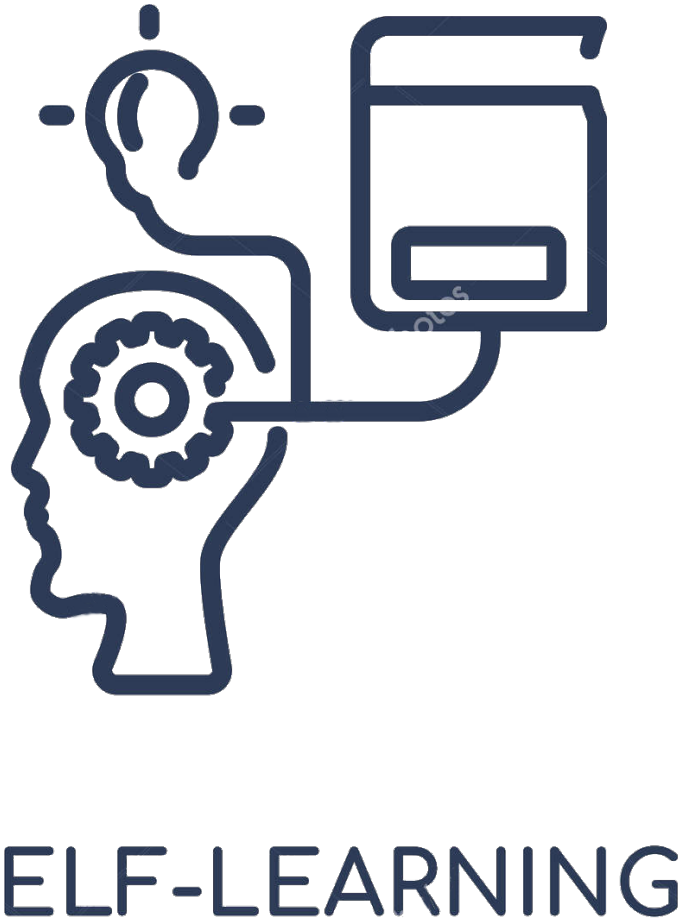


La Couche Réseau

- Adressage IP
- Protocole IP
  - Fragmentation/Réassemblage
  - Routage IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

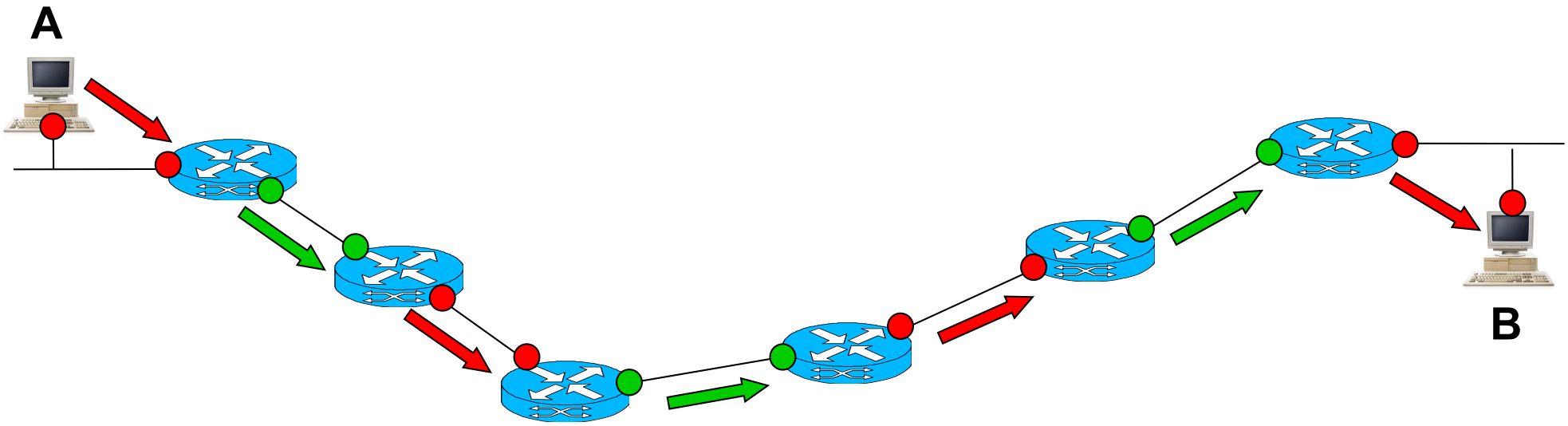
Routage IP

- Déjà vu en R101
- + Auto-apprentissage
- + Portfolio



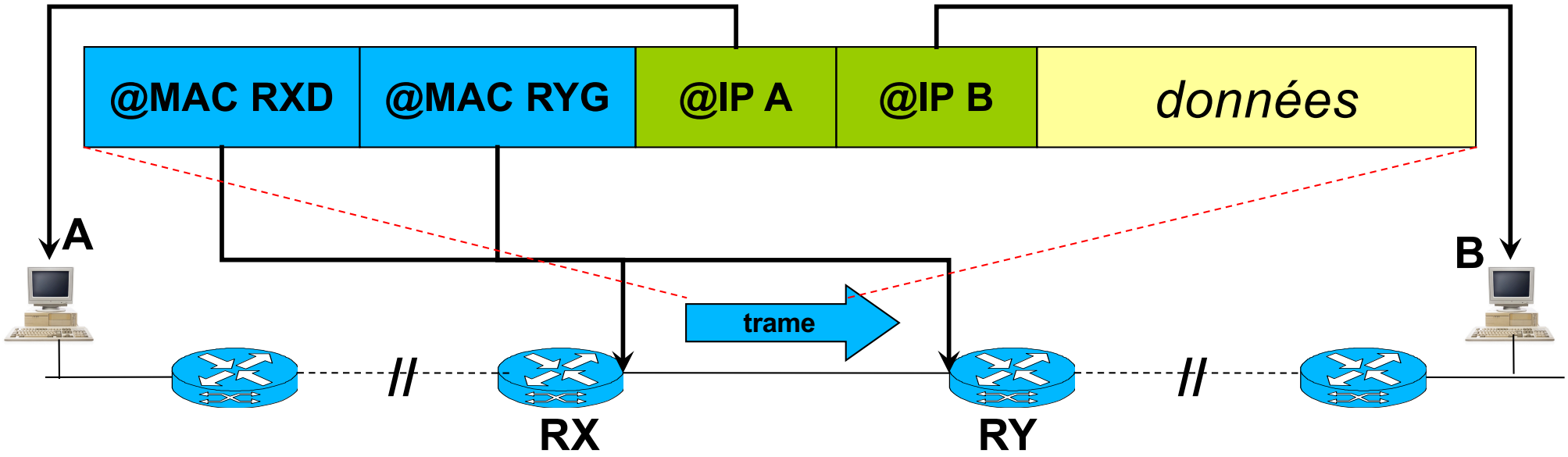
Principe général

- Un paquet est transmis au destinataire final par remises locales successives
- Dans l'exemple ci-dessous 7 remises locales sont nécessaires



Principe général

- En-têtes « accès » (Ethernet) et « réseau » (IP)



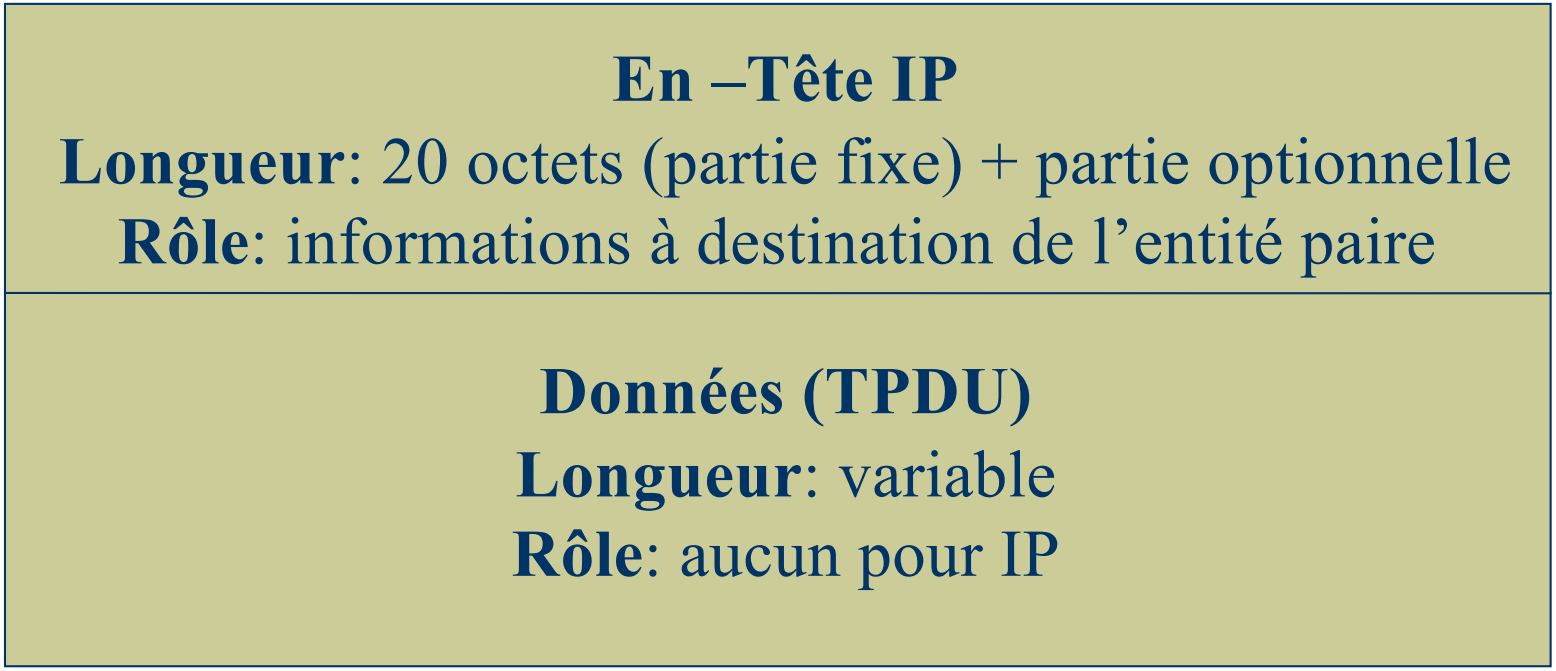
- Les adresses Source et Dest. MAC font toujours référence à **des équipements du même LAN**
- Les adresses Source et Dest. IP font toujours référence **aux équipements d'extrémité (hors NAT)**

La Couche Réseau

- Adressage IP
- Protocole IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

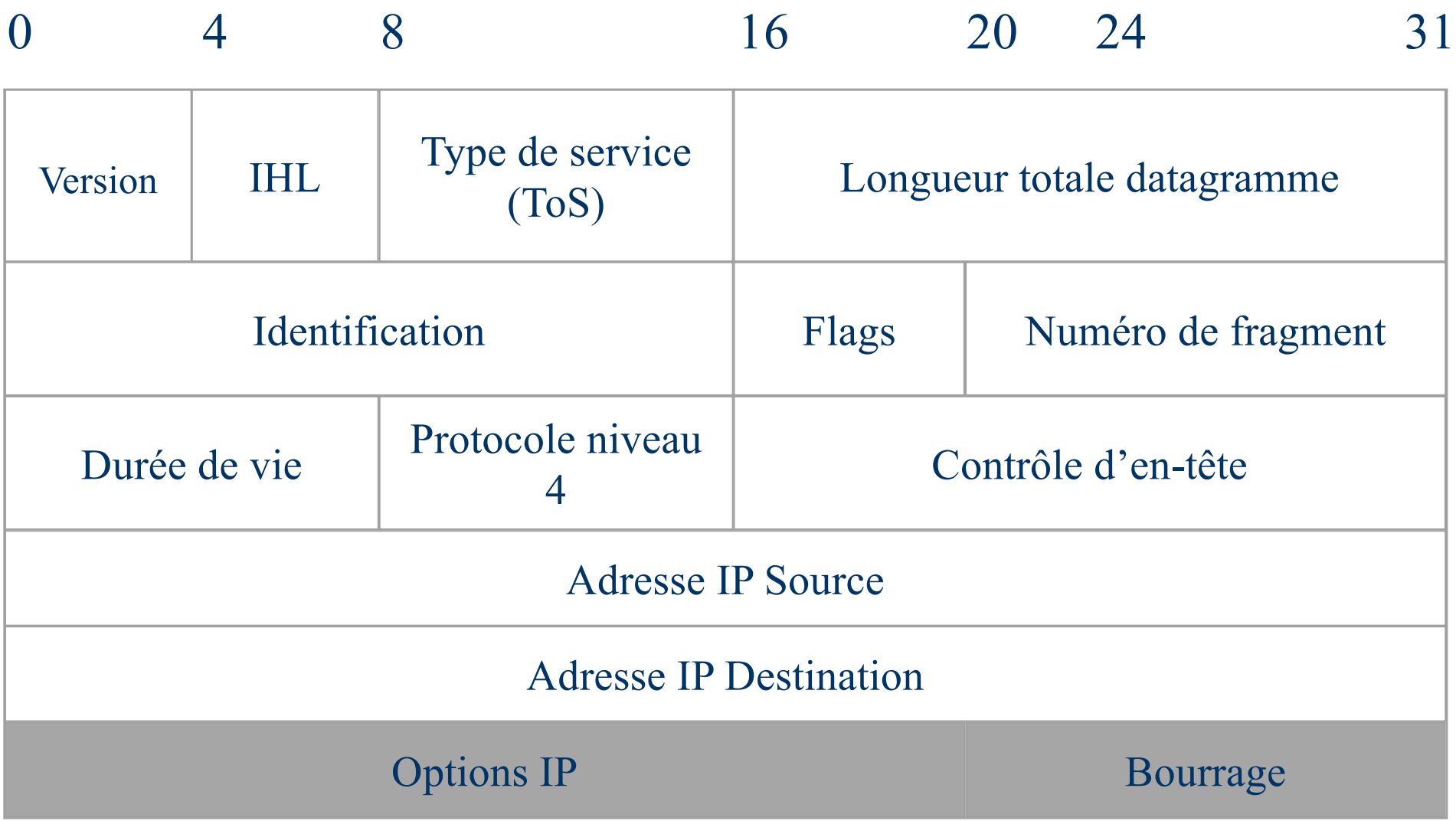
Format d'un paquet IPv4

- Deux parties:



- Taille totale maximale: 64 Koctets (2^{16}bits)

Format de l'en-tête IPv4



Format de l'en-tête IPv4

- Version (4 bits) :
  - Version du protocole IP utilisé pour construire le paquet

  ➔ possibilité de vérification de compatibilité

Format de l'en-tête IPv4

- IHL (IP Header Length, 4 bits)
  - Longueur de l'en-tête (exprimé en mots de 32 bits)

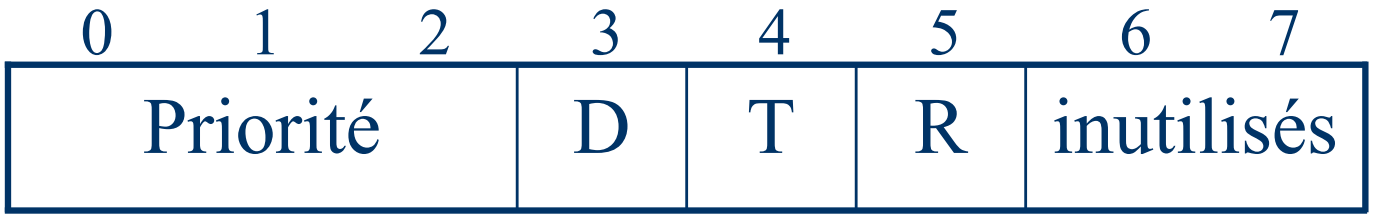
  ➔ valeur minimale 5 (5 x 4 = 20 octets), pour un paquet sans option

Format de l'en-tête IPv4

- Longueur totale (16 bits):
  - Longueur totale du paquet (en octets)
    - ➔ longueur en-tête: IHL x 4 octets
    - ➔ longueur données: Lg totale – (IHL x 4) octets
  - Valeur maximale: 65536 (64 Koctets)

Format de l'en-tête IPv4

- Type de service (ToS: Type of Service, 8bits)



- Priorité: degré de priorité du paquet

  (0: priorité normale, 7: priorité forte)

  ➔ contrôle de congestion

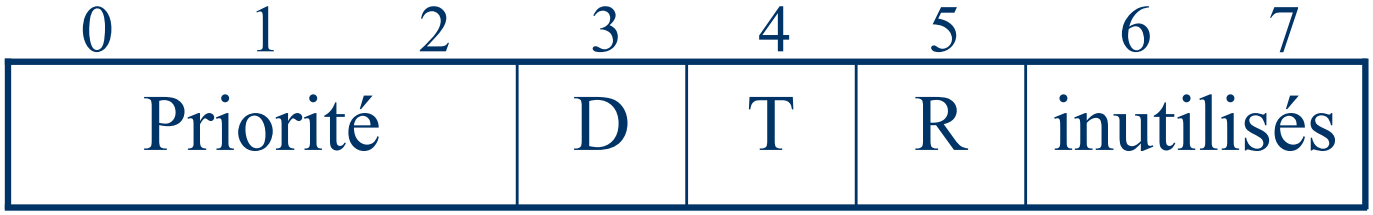
- Ce format n'est plus utilisé !

  ➔ l'utilisation de cet octet a été redéfini

  ➔ QoS (Quality of Service)

Format de l'en-tête IPv4

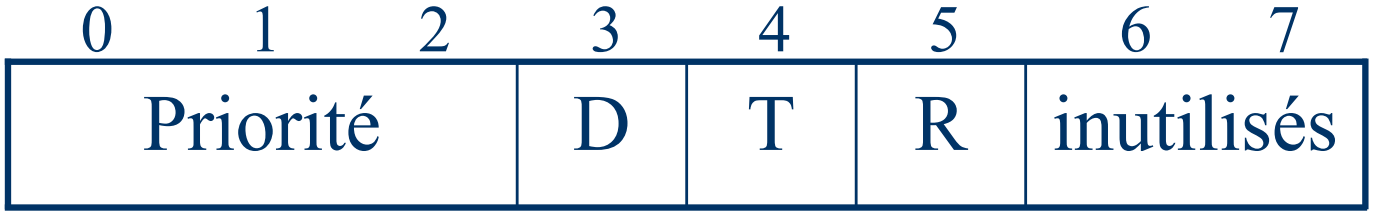
- Type de service (ToS: Type of Service, 8bits)



- Bit D: (delay) mis à 1 pour demander un court délai d'acheminement

Format de l'en-tête IPv4

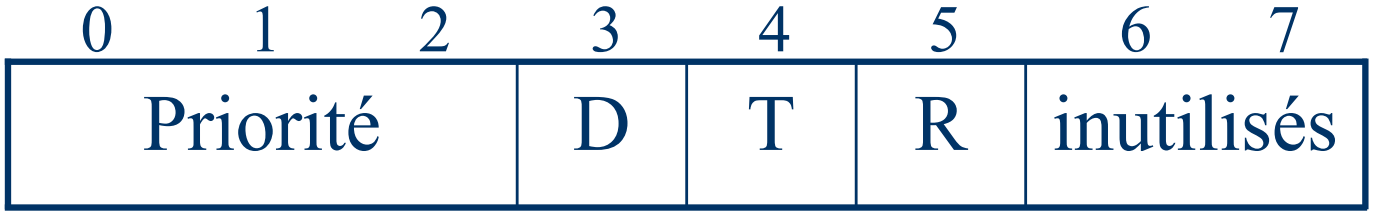
- Type de service (ToS: Type of Service, 8bits)



- Bit T: (Throughput) mis à 1 pour demander un débit élevé pour la transmission du paquet

Format de l'en-tête IPv4

- Type de service (ToS: Type of Service, 8bits)



- Bit R: (Reliability) mis à 1 pour demander un fort degré de fiabilité de transmission du dtgm
  - (ex: besoins moindres pour voix ou image)

Format de l'en-tête IPv4

- Les bits D, T, R permettent d'enregistrer des « souhaits » de la part de l'émetteur. Une prise en compte ne pourra être effective que si :
  - Plusieurs chemins existent physiquement entre les deux entités communicantes (routage multiple)
  - Plusieurs qualités de liaison existent entre les divers segments à traverser

Format de l'en-tête IPv4

- Identification (16 bits):
  - Numéro de séquence attribué par l'émetteur
  - Différent pour chaque paquet (modulo 65536)
  - Identique pour un même paquet
    - ➔ Même N° pour tous les issus fragments d'un paquet
    - ➔ Utilisé pour le réassemblage

Format de l'en-tête IPv4

- Flags (3 bits):

  - DF: (Don't Fragment)
    - mis à 1: fragmentation interdite de ce paquet
    - ➔ si impossible: paquet détruit par routeur
  - MF: (More Fragment)
    - mis à 0: dernier fragment d'un paquet
    - mis à 1: d'autres fragments suivent

Format de l'en-tête IPv4

- Numéro de fragment (Fragment Offset, 13 bits)
  - Rang du 1er octet dans le paquet N° «identification»
  - Compteur sur 13 bits (modulo 8192)
  - Valeur 0:
    - si MF=0: paquet non fragmenté
    - si MF=1: premier fragment du paquet initial

Format de l'en-tête IPv4

- Durée de Vie (TTL: Time To Live, 8 bits)
  - But: éviter les paquets qui bouclent indéfiniment
  - Valeur initiale fixée par l'émetteur
  - Chaque routeur décrémente le TTL
    - de 1, dès le début du traitement du paquets
    - de 1, à chaque seconde écoulée pendant le traitement
  - Tout paquet disposant d'un TTL nul doit être immédiatement détruit

Format de l'en-tête IPv4

- Protocole (8 bits):
  - N° officiel du protocole de niveau supérieur ayant généré le message encapsulé dans le paquet

    (RFC790: TCP = 6, UDP = 17, ICMP = 1)

    ➔ permet de déterminer à qui transmettre les données reçues

Format de l'en-tête IPv4

- Contrôle d'en-tête (16 bits)
  - « Checksum » portant sur l'en-tête IP

➔ permet une vérification rapide des en-têtes

➔ permet une vérification exclusive des en-têtes

➔ destruction du paquet en cas de valeur incorrecte

Format de l'en-tête IPv4

- Adresse IP Source (32 bits)
  - Adresse IP de l'équipement source
- Adresse IP Destination (32 bits)
  - Adresse IP de l'équipement destination

PAS D'ADRESSE IP D'EQUIPEMENT INTERMEDIAIRE

Format de l'en-tête IPv4

- Options (champ optionnel, longueur variable)
  - Utilisé pour test, mise au point, applis spécifiques, …
  - Exemples:
    - Enregistrement de route (« traceroute »)
    - Routage par la source (la source impose le chemin)
    - Horodatage (chaque routeur indique sa « notion » de temps)
    - …

Format de l'en-tête IPv4

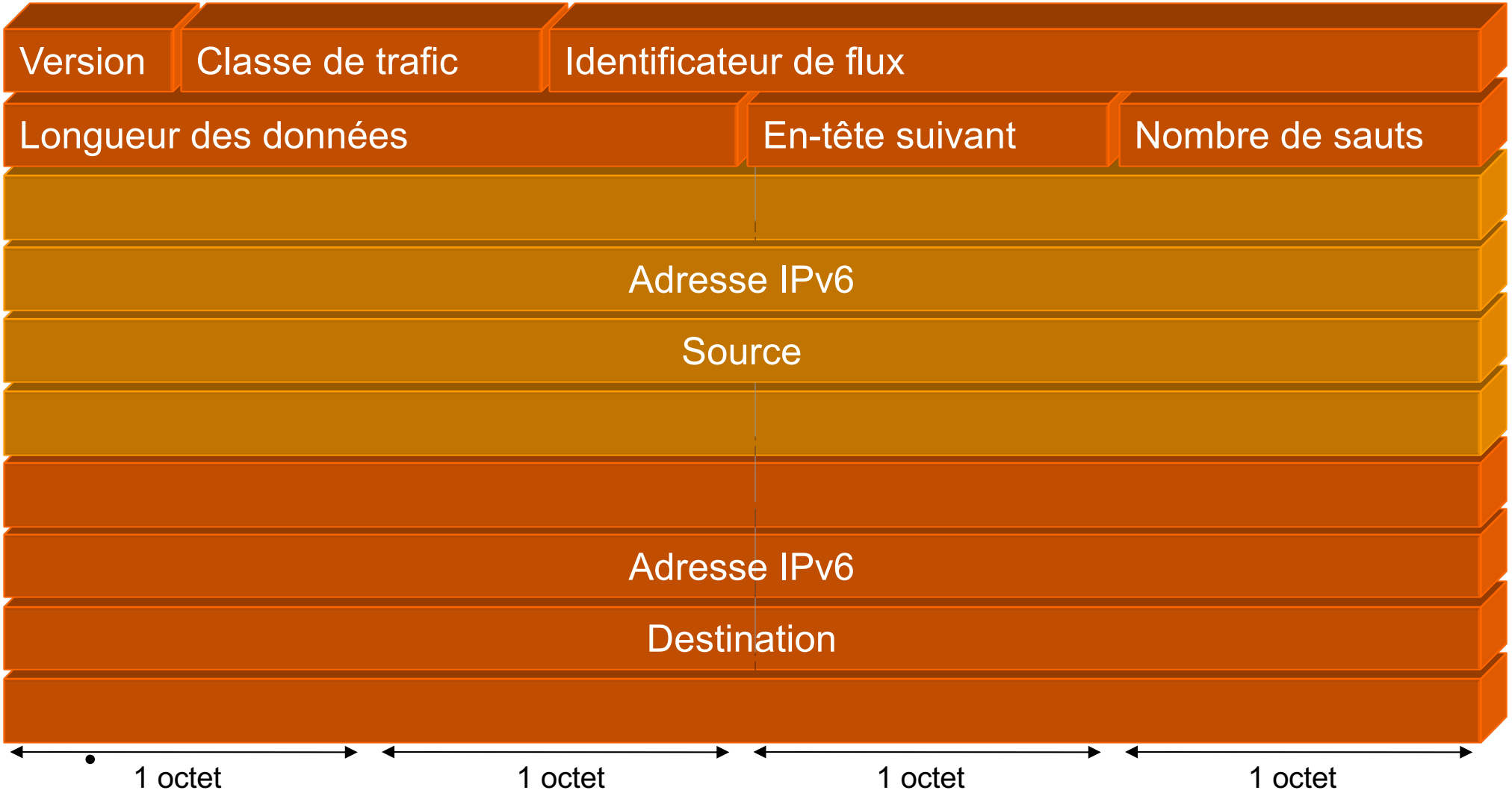
- Options (champ optionnel, longueur variable)
  - Exemple: enregistrement de route

Code option	Longueur	Pointeur	-
Adresse IP du premier nœud			
Adresse IP du deuxième nœud			
…			

Format de l'en-tête IPv4

- Bourrage (stuffing, longueur variable)
  - Comme son nom l'indique: sert à « bourrer »
  - ➔ complète un mot pour « retomber » sur 32 bits

Format de l’en-tête IPv6



Format de l'en-tête IPv6

- Identificateur de flux:
  - Nouveauté d'IPv6
  - Seul le principe est annoncé par la RFC
  - Mise en œuvre en cours d'amélioration …
  - Evite le routage de chaque paquet d'un même flux:
    - Route le premier
    - Reconnaît les suivants … et applique la même route
  - L'émetteur doit marquer tous les paquets d'un même flux avec le même identificateur

EN-TETE IPv4 vs EN-TETE IPv6

IPv4	IPv6
Version	Version
IP Header Length (IHL)	-
Type Of Service (ToS)	Classe de Trafic (Traffic Class)
-	Identificateur de Flux (FI)
Total Length (TL)	Longueur Données (Payload Length)
Identifier (ID), Flags, Fragment Offset (FO)	-
Time To live (TTL)	Nombre de Sauts (Hop Limit)
Protocol	En-tête Suivant (Next Header)
Checksum	-
Adresses Source et Destination (4 Ø)	Adresses Sources et Destination (16 Ø)

La Couche Réseau

- Adressage IP
- Protocole IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

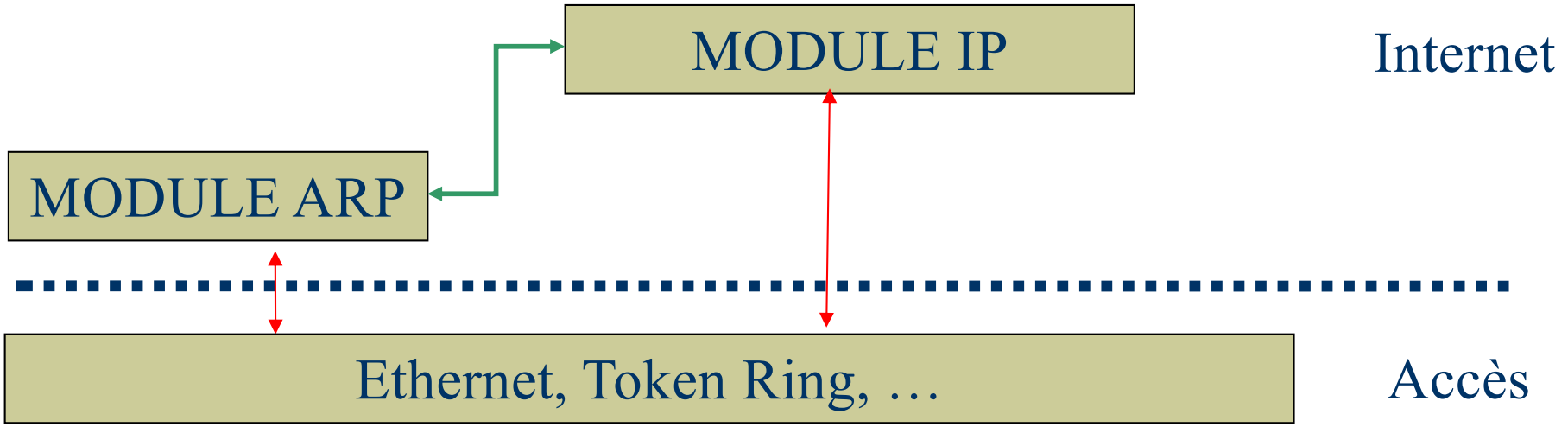
Généralités

- L'adresse IP sert à déterminer le nœud « suivant »
  - Le paquet est confié à la couche « d'accès au réseau »
  - L'adresse IP ne veut plus rien dire …
  - Il faut une adresse de niveau 2
    - Pour Ethernet: l'adresse MAC
    - Pour PPP, HDLC, … pas besoin ! C'est « l'autre » …
- Question: comment trouver l'adresse de niveau 2 ?
  - On demande LOCALEMENT « qui a l'@IP recherchée … » ?
    - **En IPv4**: à tout le monde (en broadcast)
    - **En IPv6**: au groupe de ceux qui ont une adresse IP qui finit par les trois mêmes octets que l'adresse recherchée (en multicast)

Solution IPv4: ARP

- ADDRESS RESOLUTION PROTOCOL
  - RFC 826 – 925 – 1868
  - Originellement conçu pour Ethernet 10 Mbits
  - Adaptable à d'autres technologies locales
- ARP protocole « satellite » d'IP
  - Permet d'obtenir une @MAC à partir d'une @IP
  - Permet une gestion dynamique des correspondances

Solution IPv4: ARP



: Utilise/Fournit un service au sens réseau
: Appelle/Retourne au sens fonctionnel

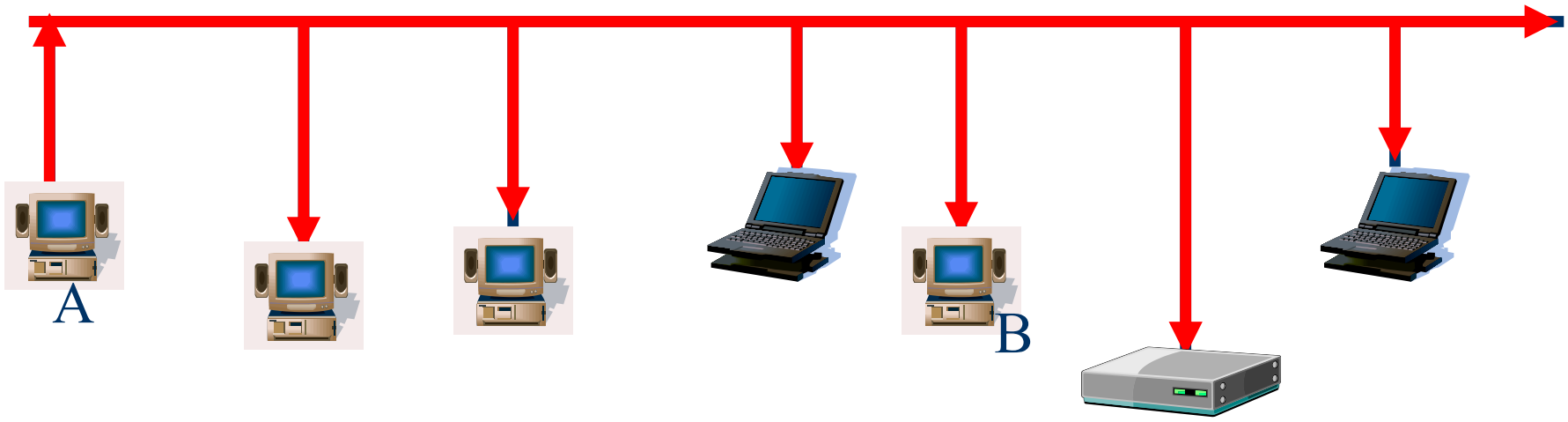
Principe de l'ARP

- Principe de fonctionnement:
  - Pb: A veut transmettre un paquet à B dont il connaît l'@IP mais pas l'@MAC

Principe de l'ARP

- 1ère phase: A diffuse une requête ARP

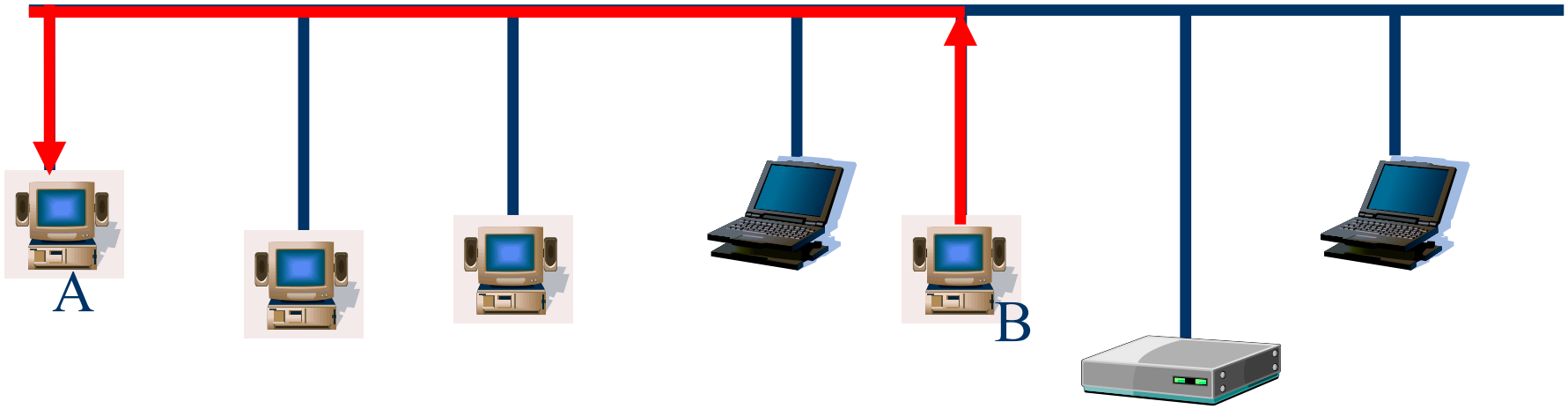
  « Qui a l'adresse @IPB ? »



Principe de l'ARP

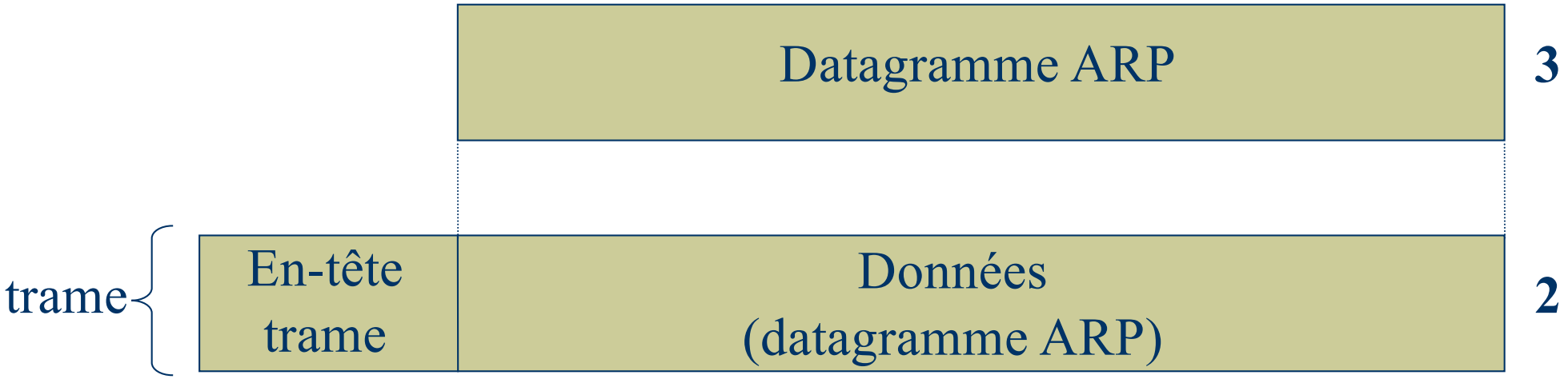
- 2ème phase: B se reconnaît et répond:

  « C'est moi: voici mon @MAC ! »

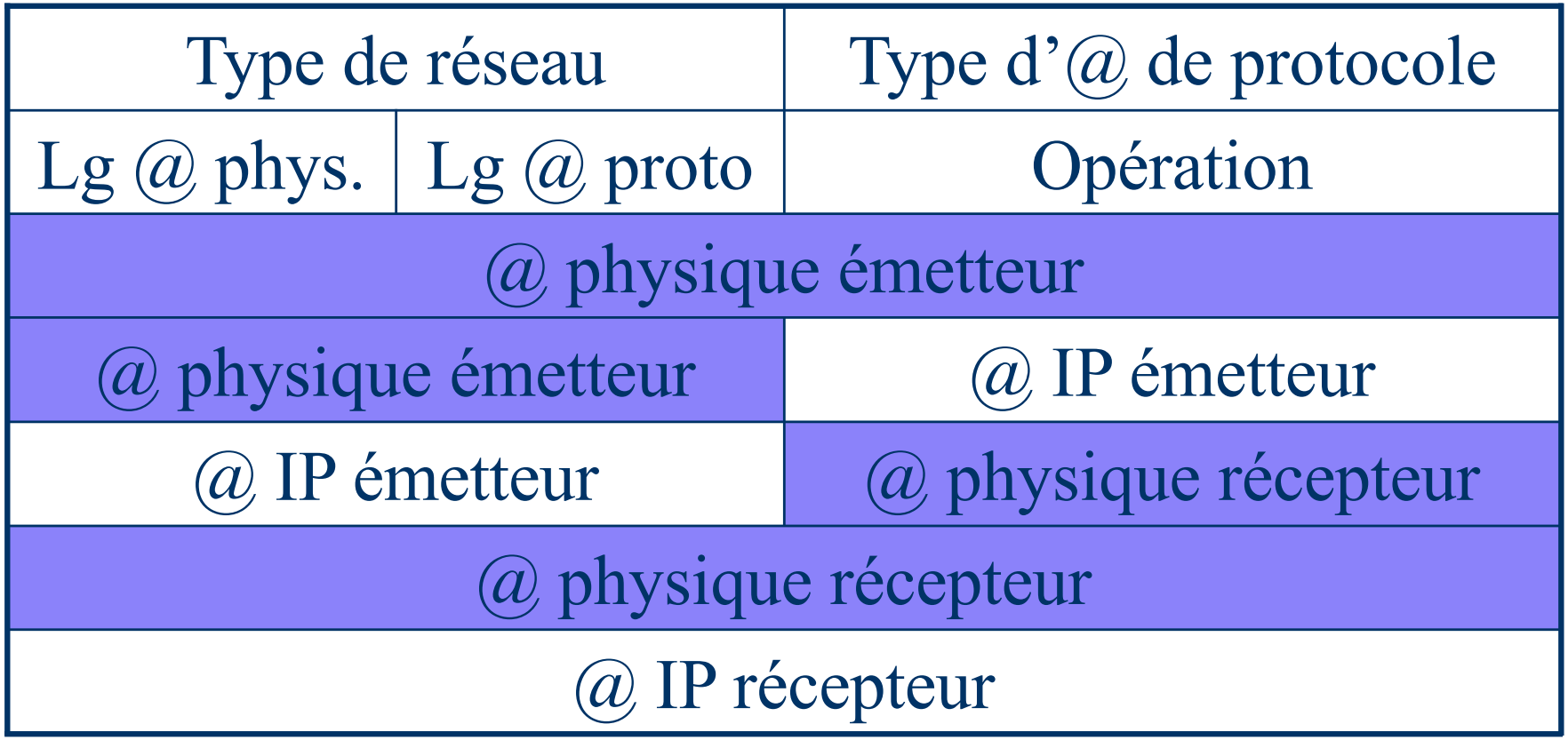


Datagramme ARP

- Encapsulation dans les trames de liaison :



Format datagramme ARP



Format datagramme ARP

- Type de réseau (16 bits):
  - Type de réseau sur lequel le datagramme est transmis (ex: 0001 pour Ethernet)
- Type d'@ de protocole (16 bits):
  - Type d'adresse de niveau 3 (ex: 0800 pour IP)

Format datagramme ARP

- Longueur @ Physique (8 bits):
  - Longueur en octets de l'adresse physique (ex: 6 pour une adresse MAC Ethernet)
- Longueur @ Protocole (8 bits):
  - Longueur en octets de l'adresse de niveau 3 (ex: 4 pour une adresse IP)

Format datagramme ARP

- Opération (16 bits):
- Code de l'opération

  Ex: 0001: requête ARP

  0002: réponse ARP

Format datagramme ARP

- Requête:

@MAC SOURCE @ MAC A	@IP SOURCE @IP A
@MAC DESTINATION *Sans objet*	@IP DESTINATION Question @ IP B

Format datagramme ARP

- Réponse:

@MAC SOURCE Réponse: @ MAC B	@IP SOURCE @IP B
@MAC DESTINATION @ MAC A	@IP DESTINATION @ IP A

Optimisation du Protocole

- Cache ARP :
  - Chaque équipement dispose d'une table locale
  - 1 entrée = 1 correspondance (@IP , @MAC)
  - Si l'@MAC du destinataire est déjà dans le cache:
    - ➔ pas d'émission de requête ARP
    - ➔ gain de temps notable
    - ➔ pas d'encombrement superflu du réseau

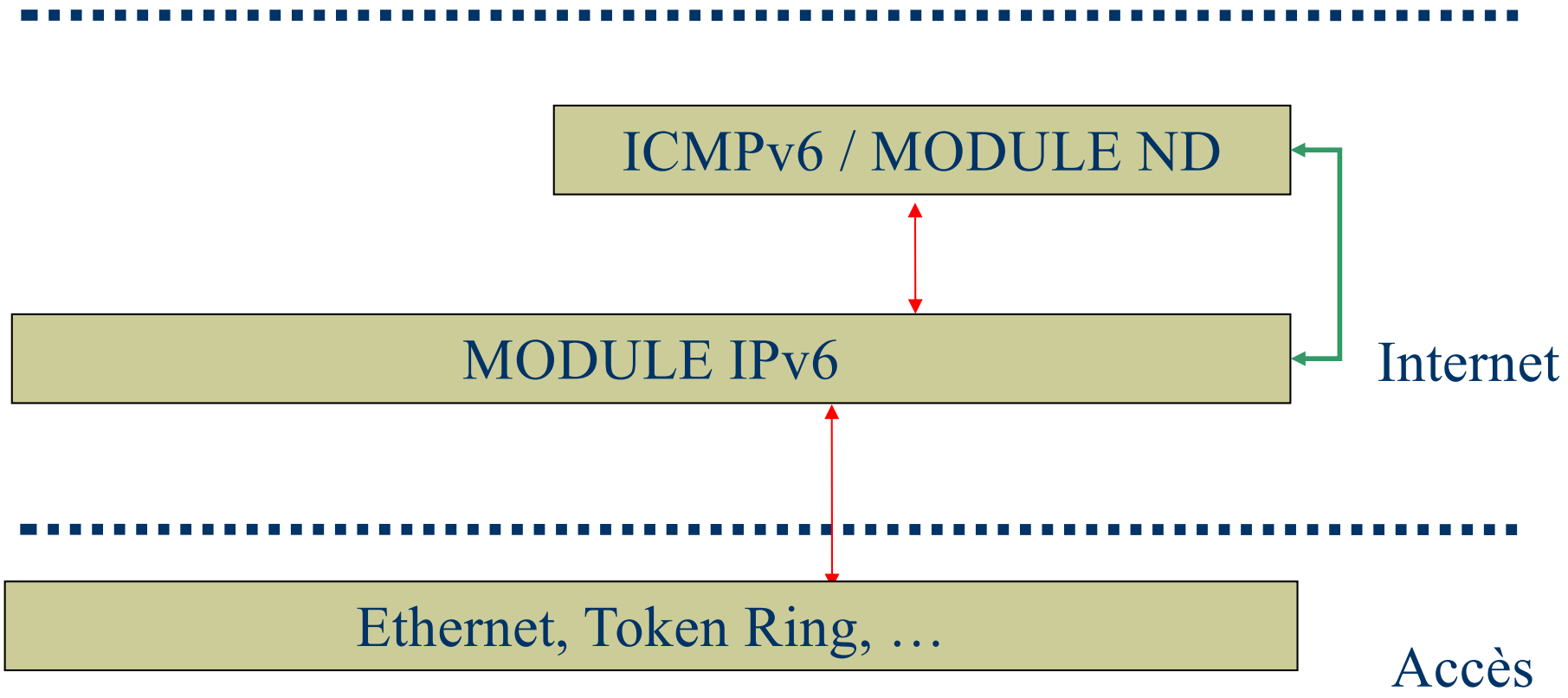
Optimisation du Protocole

- Gestion dynamique du cache ARP :
  - Ajout d'une entrée dans le cahe:
    - A chaque réception de réponse
    - A chaque réception de requête (même sans être concerné)
  - A chaque démarrage toute machine envoie une requête
    - « ARP gratuit » (« gratuitous ARP »)

    ➔ mise à jour de tous les caches du réseau
  - Suppression automatique d'une entrée après qq secondes
  - Annulation de tout le cache à chaque redémarrage

➔ Evolution rapide des caches ARP

Solution IPv6: ND



: Utilise/Fournit un service au sens réseau
:Appelle/Retourne au sens fonctionnel

Solution IPv6: ND

- ND: Neighbour Discovery (fonctionnalité d'ICMPv6)
- En IPv6 : pas de broadcast..
- Multicast à l'attention de « l'adresse de multicast d'un nœud »
  (« sollicited node multicast »)

- L'adresse de multicast d'un nœud est constituée du préfixe **FF02:** auquel on colle le suffixe **1:FF** suivi des 3 derniers octets de l'adresse IPv6 du nœud

- Exemple :
  - Pour l'équipement **FE80::211:43FF:FE14:4211**
    L'adresse de multicast du nœud sera :
  - **FF02::1:FF14:4211**

Proxy NDP IPv6

- Principe identique pour IPv6
  - Même principe
  - Mêmes avantages
  - Mêmes inconvénients
- Une GROSSE difficulté supplémentaire:
  - En IPv4 le proxy reçoit les demandes en Bcast
  - En IPv6, il doit être abonné à TOUS les groupes multicast correspondants …

    ➔ nécessité d'un « Multicast Discovery Protocol »

La Couche Réseau

- Adressage IP
- Protocole IP
- Protocole ARP
- Routage IP
- Protocole ICMP
- Synthèse de fonctionnement

Généralités

- Internet Control Message Protocol
  - IPv4: RFC 792
  - IPv6: RFC 4443
- Protocole de niveau 3, « au dessus » d'IP
- 2 Rôles:
  - Générer des messages de contrôle IP
    - ex: Hôte destination injoignable, pas de réseau, …
  - Générer des messages de supervision
    - ex: ping (v4 ou v6), ND (v6)

Généralités

- Caractéristiques
  - obligatoire dans toute mise en œuvre de IP
  - transmet des messages de contrôle (ou de supervision) entre les couches IP de deux équipements
  - Messages de contrôle: compte rendus d'erreur uniquement (pas de correction)
  - Informe (éventuellement) le protocole de niveau 4

Messages de contrôle

- Message de contrôles = causes d'erreurs
- Causes de déclenchement diverses:
  - Panne de liaison

  ➔ pas de réseau,…
  - Destinataire physiquement déconnecté

  ➔ hôte destinataire inexistant, arrêté, en panne, …
  - Expiration de la durée de vie d'un datagramme

  ➔ Destruction d'un paquet sur TTL v4 (Hop limit v6) à 0
  - Service non disponible

  ➔ La machine répond mais le port correspondant est fermé
  - …

Messages de contrôle

- Caractéristiques d'un message de contrôle:
  - Destinataire ?

➔ Toujours l'expéditeur du paquet responsable de l'erreur

  - Contenu ?

➔ Une description du problème rencontré

Messages de Supervision

- Quelques exemples:
  - Tests d'accessibilité (ping)

    ➔ Vérification de l'activité IP d'un équipement
  - Contrôle de congestion

    ➔ Demande d'arrêt temporaire d'émission entre routeurs (file d'attente d'entrée qui sature)
  - Redirection de routes

    ➔ Proposition d'une autre passerelle
  - …

Messages de supervision

- Caractéristiques d'un message de supervision:
  - Destinataire ?

➔ variable !

  - Contenu ?

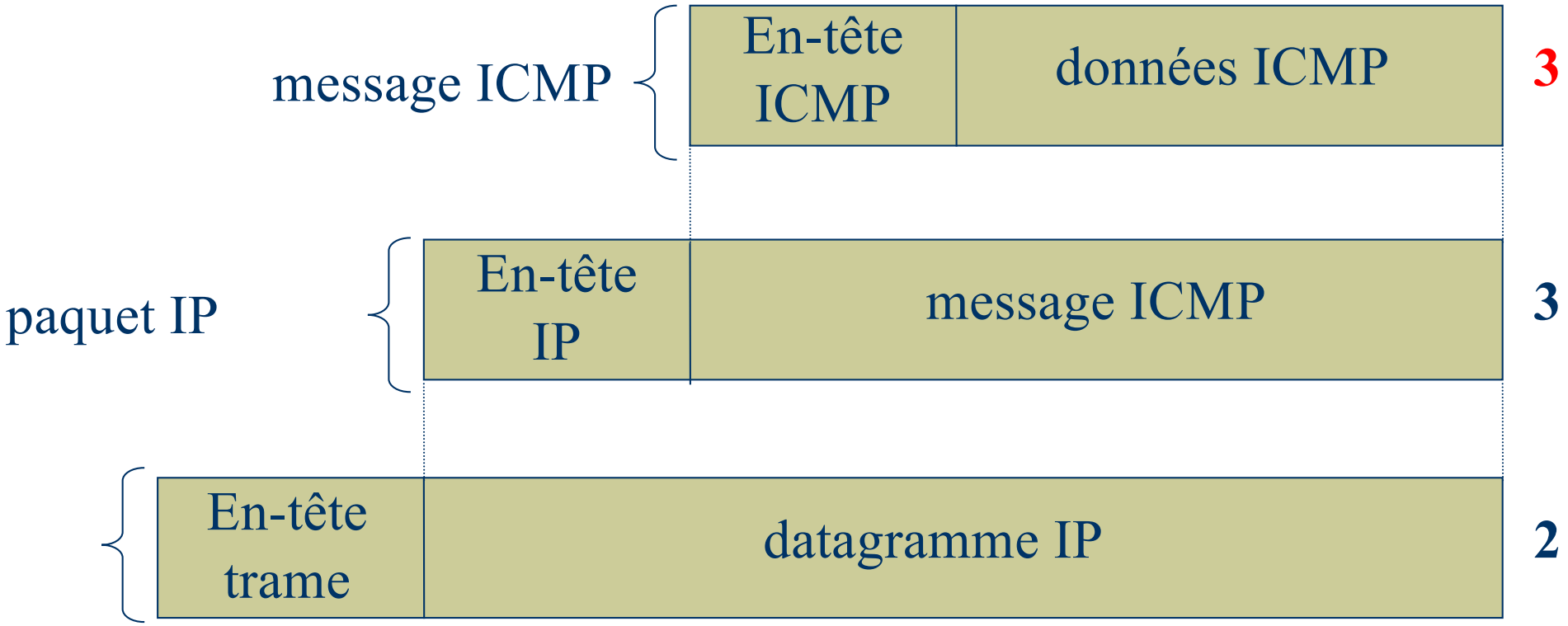
➔ différent selon type

Messages ICMP

- Acheminés par des paquets IP classiques
  - ➔ pas de priorité particulière
- Pertes ou destruction de messages ICMP …
  - ➔ Pas de génération de message ICMP … !!!

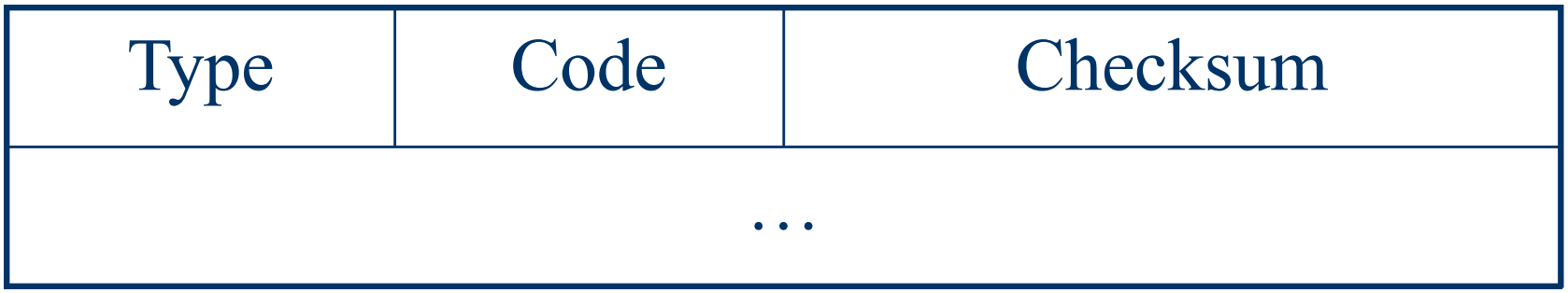
Format des messages ICMP

- Encapsulation dans un paquet IP :



Format des messages ICMP

- Format différent pour chaque type
- Trois premiers champs communs (4 octets)



Format des messages ICMPv4

- Type (1 octet)
  - 0: Réponse Echo
  - 3: Destination non accessible
  - 4: Contrôle de flux
  - 5: Redirection de route
  - 8: Echo
  - 11: Durée de vie écoulée
  - 12: Erreur de paramètre
  - 13: Marqueur temporel
  - 14: Réponse à un marqueur temporel
  - 15: Demande d'information
  - 16: Réponse à une demande d'information

Format des messages ICMPv4

- Code (1 octet)
  - Équivaut à un « sous-type »
  - Variable selon le champs « Type »
  - Ex: pour le type 3 (destination non accessible)
    - 0: réseau non accessible
    - 1: hôte non accessible
    - 2: protocole non accessible
    - 3: port non accessible
    - 4: fragmentation nécessaire mais interdite
    - 5: échec d'acheminement source

Format des messages ICMPv4

- Checksum (2 octets)
  - Somme de contrôle sur la totalité du message
  - Le champs « checksum » est maintenu à 0 pour le calcul du checksum, et renseigné ensuite

Exemple de message ICMPv4

- Type 0 ou 8: « ping » ou « réponse au ping »
- Code 0 (pas de sous type)

0 ou 8	0	Checksum
Identificateur		Numéro de séquence
Données optionnelles (octets à renvoyer dans la réponse)		

- identificateur et n°de séquence: permettent de mettre en relation requêtes et réponses
- données optionnelles: permettent d'alourdir le message

Exemple de message ICMPv4

- Type 3: « destinataire non accessible »
- Code 1: « hôte inaccessible »

3	1	Checksum
non utilisé		
Paquet original (en-tête IP + 64 premiers bits)		

- (Les 64 premiers bits sont censés contenir un éventuel numéro de port utilisé par le protocole de niveau 4)

Format des messages ICMPv6

- Les messages ICMPv6 ont le même format que les messages ICMPv4
- Les fonctionnalités sont différentes

➔ les valeurs du champ « type » aussi …

Format des messages ICMPv6

- Type (1 octet)
  - 1: Destination non accessible
  - 2: Paquet trop grand
  - 3: Durée de vie écoulée
  - 4: Problème de paramètres
  - 128: Echo (Echo Request) = PINGv6
  - 129: Réponse à l'Echo (Echo Response) = PONGv6
  - 130: Requête en appartenance de groupe (Membership Group Rq)
  - 131: Réponse en appartenance de groupe (Membership Group Rp)
  - 132: Réduction d'une appartenance de groupe (Mb. Gr. Reduction)
  - 133: Sollicitation de routeur (Router Solicitation)
  - 134: Information d'un routeur (Routeur Advertisement)
  - 135: Sollicitation de voisin (Neighbour Solicitation)
  - 136: Information d'un voisin (Neighbour Advertisement)

La Couche Réseau

- Adressage IP
- Protocole IP
- En-Tête IP
- Protocole ARP (v4) ou ND (v6)
- Protocole ICMP
- Synthèse de fonctionnement

Schéma Récapitulatif IPv4

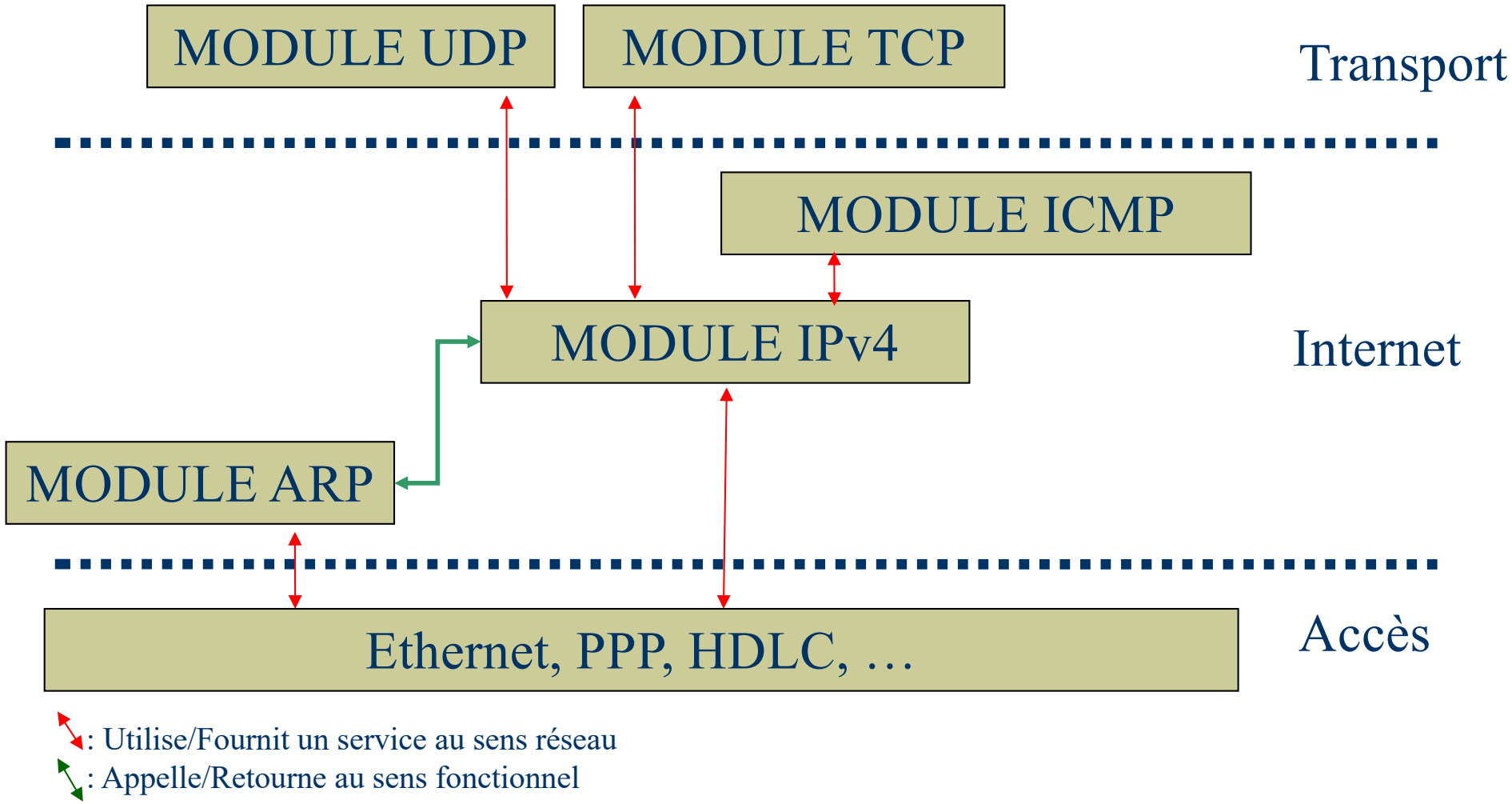
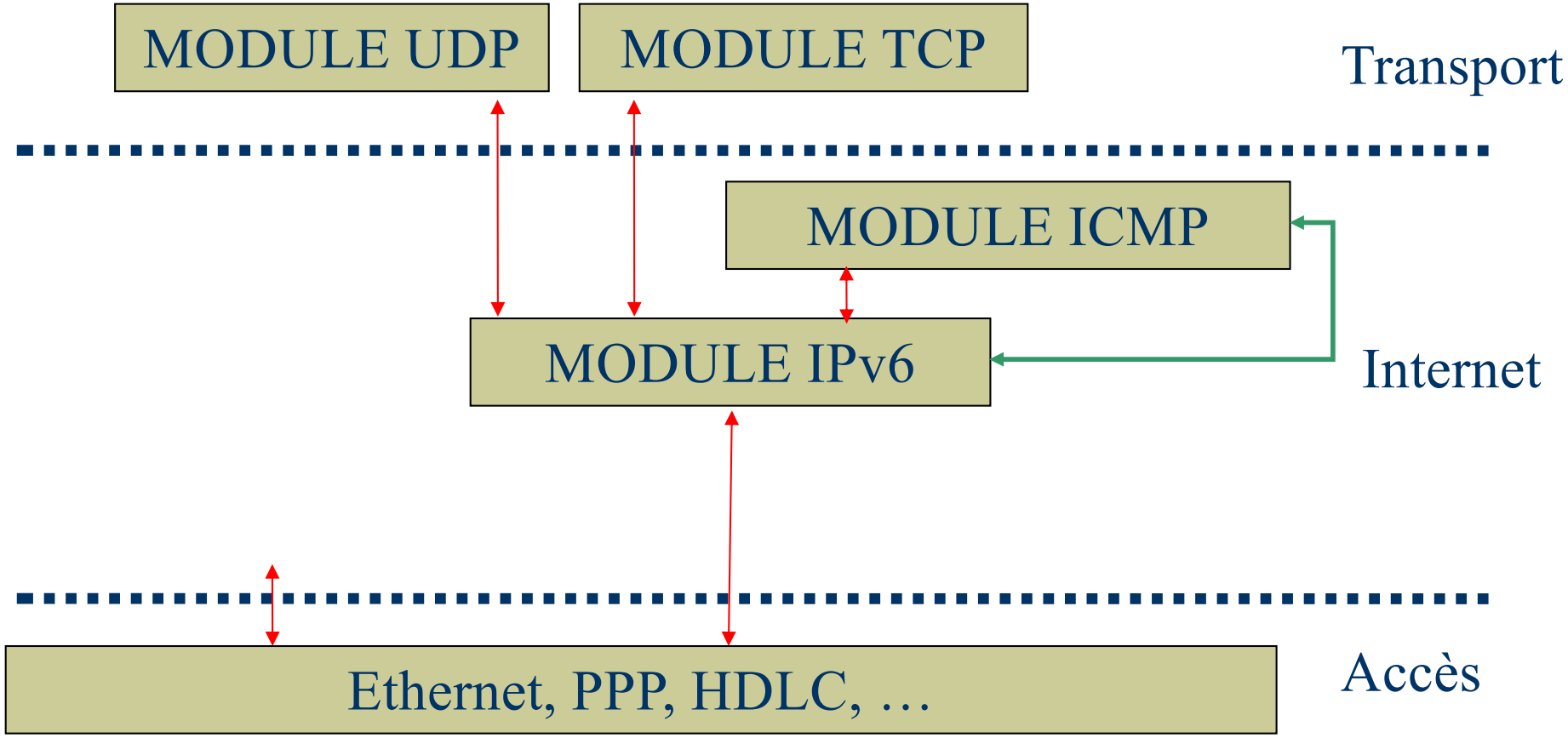


Schéma Récapitulatif IPv6



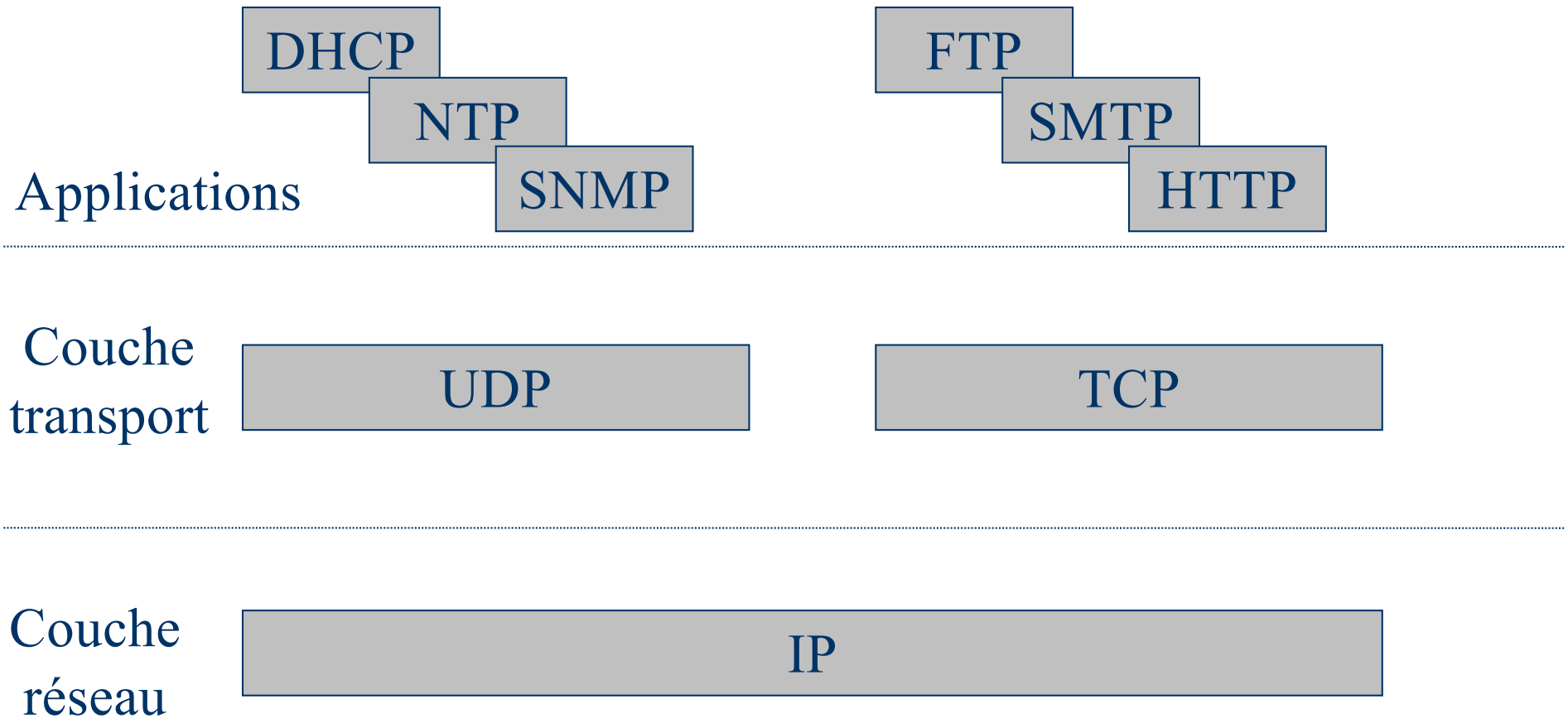
Transport dans le modèle TCP/ IP

- Introduction
- Notion de port
- TCP/UDP: mécanismes communs
- Le protocole UDP
  - Format de l'en-tête
- Le protocole TCP
  - Gestion d'une connexion (ouverture, relâchement, réinitialisation)
  - Contrôle de flux
  - Format de l'en-tête

Objectifs

- Transfert de bout en bout (end to end)
  - Pas de pb d'acheminement
  - Pas de visibilité d'hétérogénéité de réseaux
- Utilise les services de IP (client de IP)
- Fournit des services à ses clients
  - Généralement des services de niveau applicatif

Architecture



Protocoles

- Deux protocoles:
  - User Datagram Protocol (UDP - rfc 768)
    - Service en mode non connecté
    - Remise non fiable
  - Transmission Control Protocol (TCP – rfc 793)
    - Service en mode connecté
    - Remise fiable

Notion de « Port »

- Rôle: Identifier les applications clientes de Transport
  - 1 @ IP = 1 équipement = X applications

  ➔ nécessité d'une adresse complémentaire

  ➔ 1 port = 1 @ d'application

Notion de « Port »

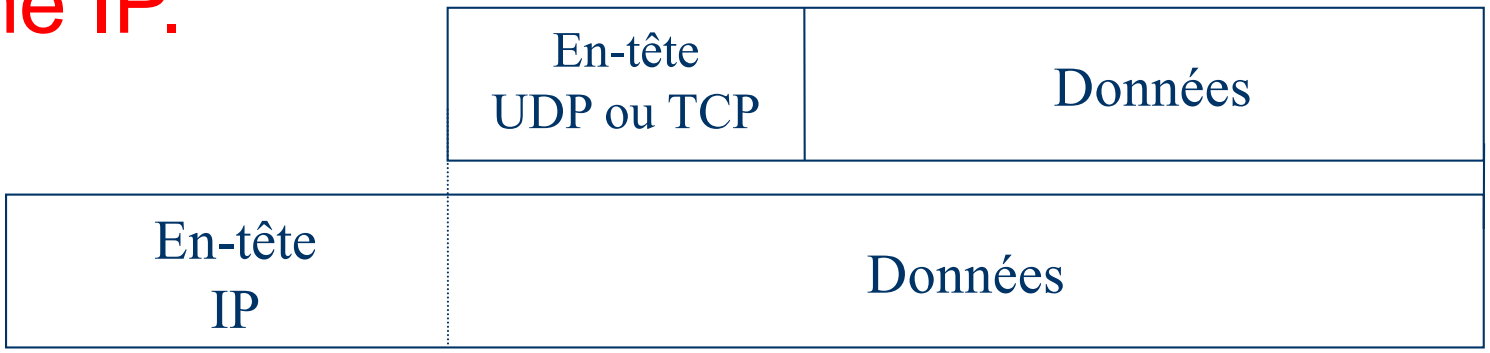
- Mise en œuvre:
  - 1 port = 1 nbre entier = 1 processus applicatif réseau
  - De 0 à 1023: ports réservés
    - applications standardisées (rfc 1700)
    - Droits « superviseur » nécessaires
  - Association « Service/Port »:
    - Statique: cas des processus serveur (/etc/services sous Unix)
    - Dynamique: cas des processus clients. Port attribué par le mécanisme des « sockets ».

Notion de « Port »

- Conséquences:
  - Association d'applications: une association entre deux processus d'application (souvent client et serveur) peut être décrite par 5 paramètres:
    - @ IP source
    - @ IP destination
    - @ appli source (Port source)
    - @ appli destination (Port Destination)
    - Protocole de transport (UDP ou TCP)

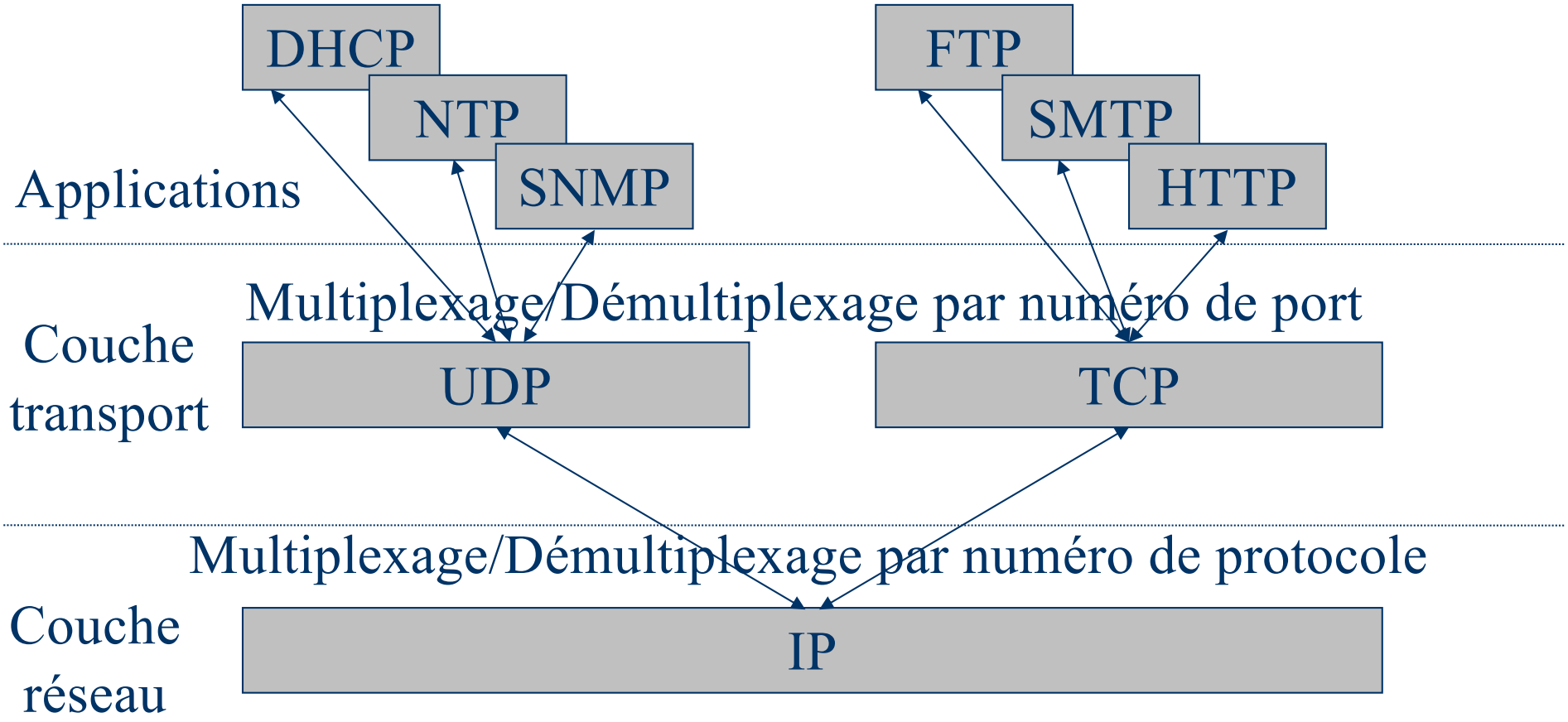
Encapsulation des messages

- Message UDP ou TCP encapsulé dans un dtgme IP.



- Différence: champs « protocole » de l'en-tête IP
  - UDP: 17
  - TCP: 6

Multiplexage / Démultiplexage



Le protocole UDP

- Caractéristiques générales:
  - Faible complément de services à IP:
    - Identification de l'application (port)
    - Calcul de checksum (un plus pour IPv6)

    ➔ élément essentiel pour le démultiplexage sur port
  - Les faiblesses de IP se retrouvent:
    - Pertes, duplications, retard, déséquencement possibles

    ➔ les applications clientes doivent les prendre en charge

Le protocole UDP

- Format d'un datagramme UDP

Port Source	Port Destination
Longueur	Checksum UDP
Données	

  - Port source: (16 bits)
    - Adresse facultative de l'application émettrice
  - Port destination: (16 bits)
    - Adresse de l'application destinataire
  - Longueur: (16 bits)
    - Longueur totale du message UDP
  - Checksum UDP: (16bits)
    - Champ à 0 si non utilisé (IPv4), valeur du checksum sinon

Le protocole TCP

- Caractéristiques générales
  - Importants compléments de services à IP
    - Transfert fiable de bout en bout
    - Transfert en mode connecté (circuit virtuel)
  - Mode connecté
    - Établissement de connexion
    - Exploitation de la connexion
    - Relâchement de la connexion

Le protocole TCP

- Caractéristiques générales
  - Message TCP = segment TCP
  - Transfert fiable
    - Contrôle de la fiabilité des données (altération, dupli)
    - Numérotation et acquittement (reséquencement, pertes)
  - De bout en bout
    - Transport n'agit que sur les équipements terminaux. Le routage et le réseau deviennent transparents
  - Full Duplex
    - Echange simultané de deux flux bidirectionnels

Le protocole TCP

- Caractéristiques générales
  - Orientation « flot d'octets »
    - TCP gère les données au niveau de l'octet et non du segment
  - Contrôle de flux
    - Mécanisme de « sliding windows » par anticipation
  - Niveaux de priorité
    - Existence de données urgentes (express)
  - Mode tamponné
    - TCP tamponne les données en blocs avant de les faire remonter au client

Gestion de connexion

- Gestion d'une connexion
  - 3 opérations possibles:
    1- Etablissement d'une connexion
    2- Exploitation de la connexion
    3- Relâchement normal d'une connexion

    ou

    3- Réinitialisation d'une connexion (abandon immédiat)

Ouverture de connexion

- Etablissement actif ou passif d'une connexion
  - Ouverture ACTIVE (généralement côté « client »)

  ➔Le processus initiateur demande à TCP une ouverture active de connexion sur le processus distant
    - Un PORT local de connexion est attribué dynamiquement par le système d'exploitation (au dessus de 1023)
    - TCP envoie une demande par réseau à l'entité distante SUR LE PORT CONVENTIONNEL DU SERVEUR
    - Lorsqu'une réponse est reçue de l'entité distante, TCP transmet une confirmation au processus client

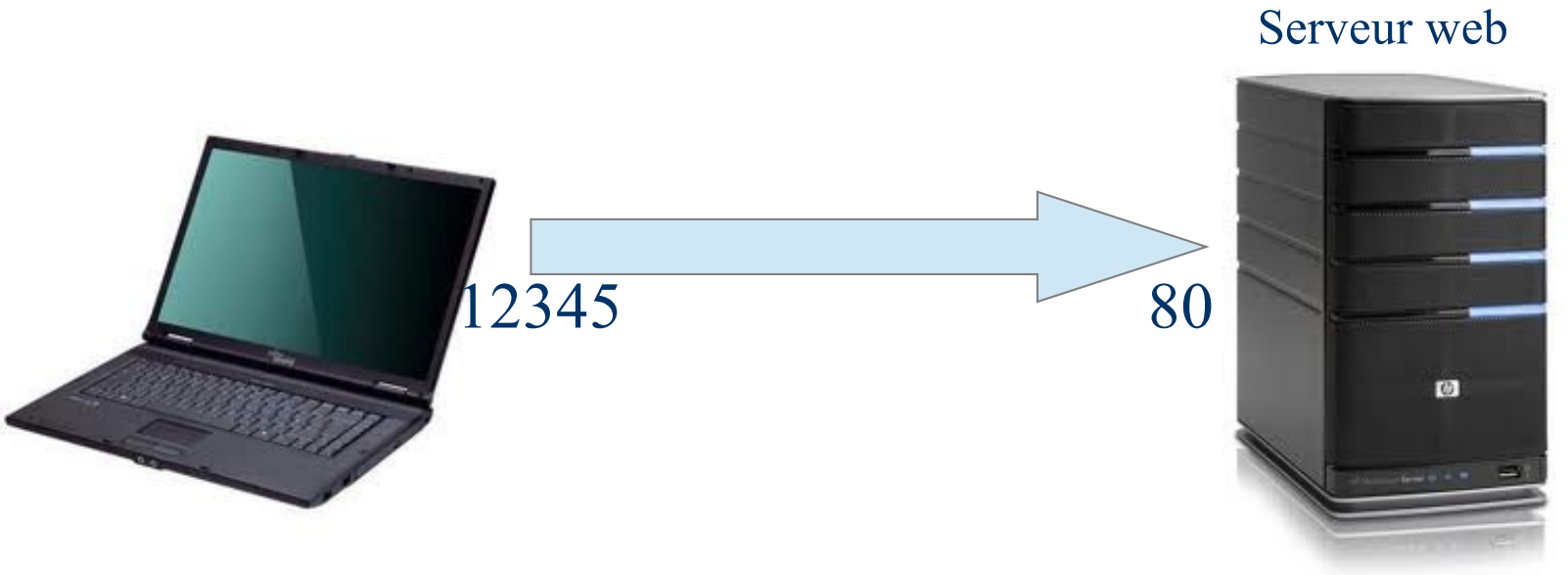
Ouverture de connexion

- Etablissement actif ou passif d'une connexion
  - Ouverture PASSIVE (généralement côté « serveur »)

  ➔Le processus répondant autorise TCP à accepter une connexion entrante
    - Le processus « serveur » demande à TCP d'autoriser les demandes de connexion entrantes sur un PORT CONVENTIONNEL
    - Le processus et le port correspondant sont « bloqués » à l'écoute d'une demande de connexion entrante

Ouverture de connexion

- A l'initiative du client :



Port client (aléatoire):
12345

Port serveur (conventionnel):
80

Ouverture de connexion

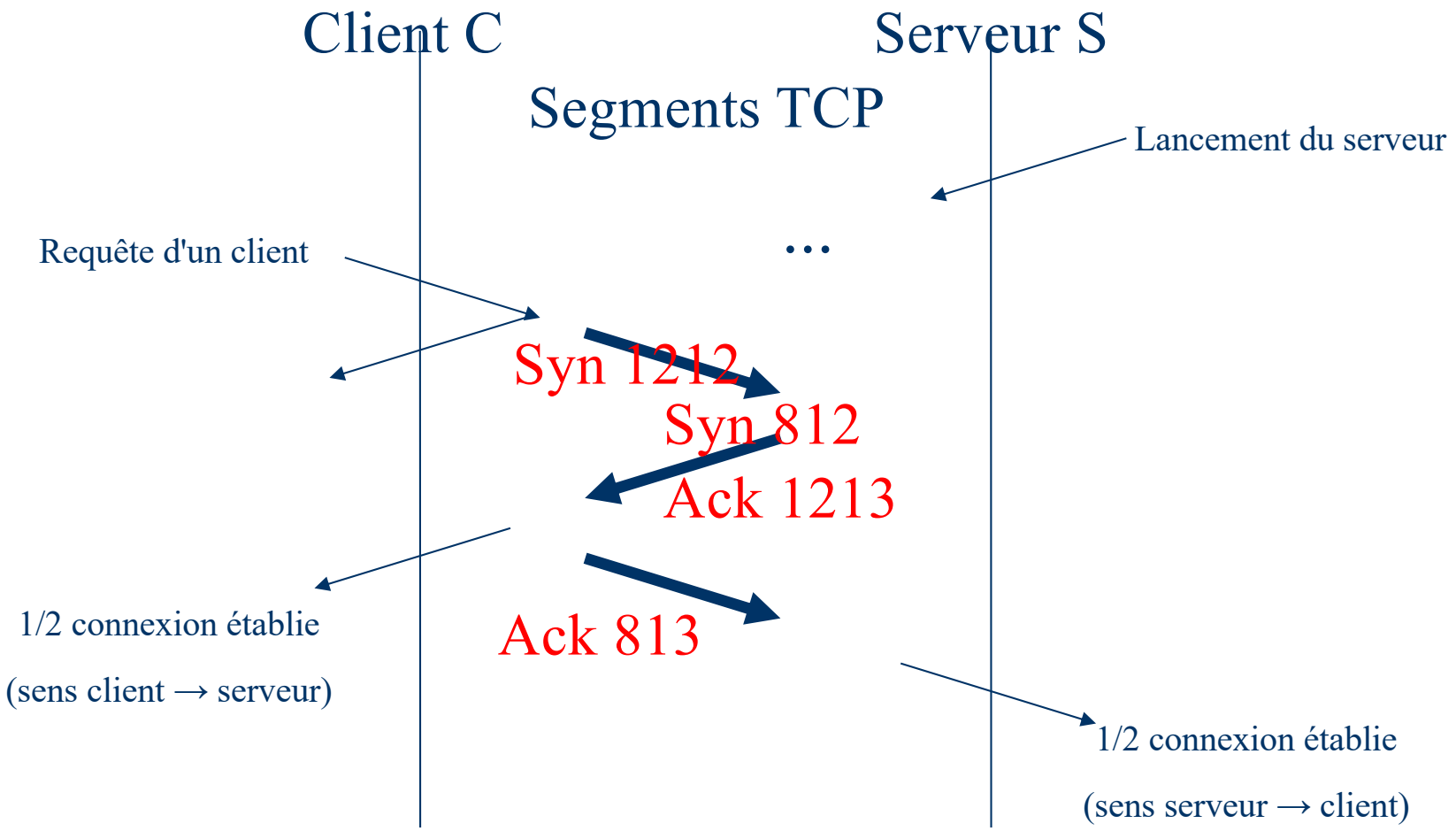
- Synchronisation des numéros de séquence
  - Des numéros de séquence sont utilisés pour le reséquencement des messages ainsi que pour les acquittements.
  - TCP étant Full duplex, il faut deux systèmes de numérotation. Il faut donc connaître le numéro de séquence initial (ISN) utilisé par l'entité paire
  - On ne commence pas à zéro pour des raisons de fiabilité et surtout de sécurité.

  ➔ Une synchronisation est effectuée lors de l'établissement de la connexion

Ouverture de connexion

- Ouverture de connexion: 3 phases
  - C envoie à S un segment de demande d'ouverture de cx. C transmet en même temps sa valeur d'ISN: X
  - S reçoit la requête, enregistre ISNc. Elle répond par un segment en acquittant le ISN X et transmet son propre ISN: Y
  - C reçoit le segment, enregistre le ISN Y de S et répond en acquittant le ISN Y

Ouverture de connexion



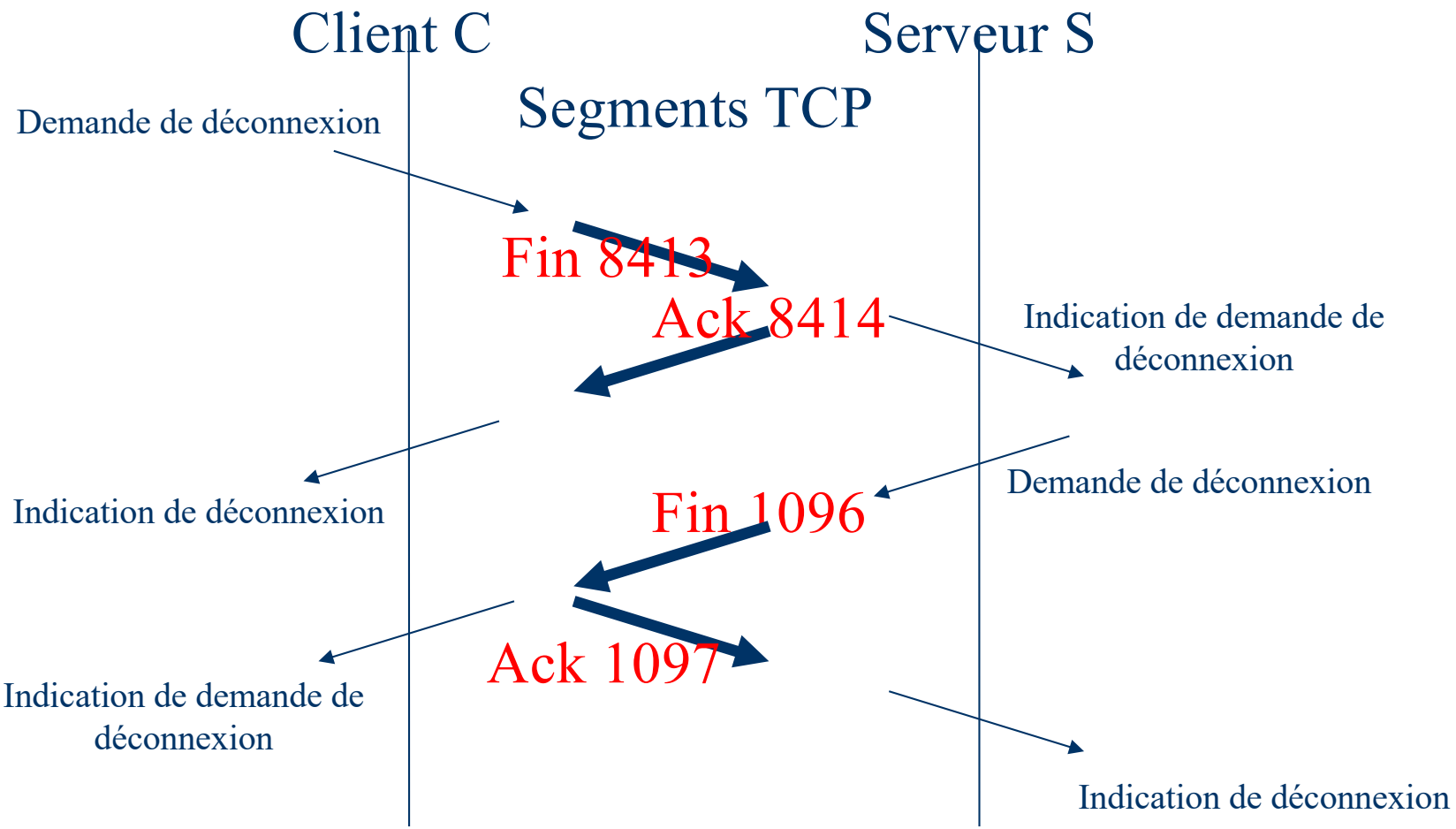
Relâchement de connexion

- Relâchement normal de connexion: 3 phases

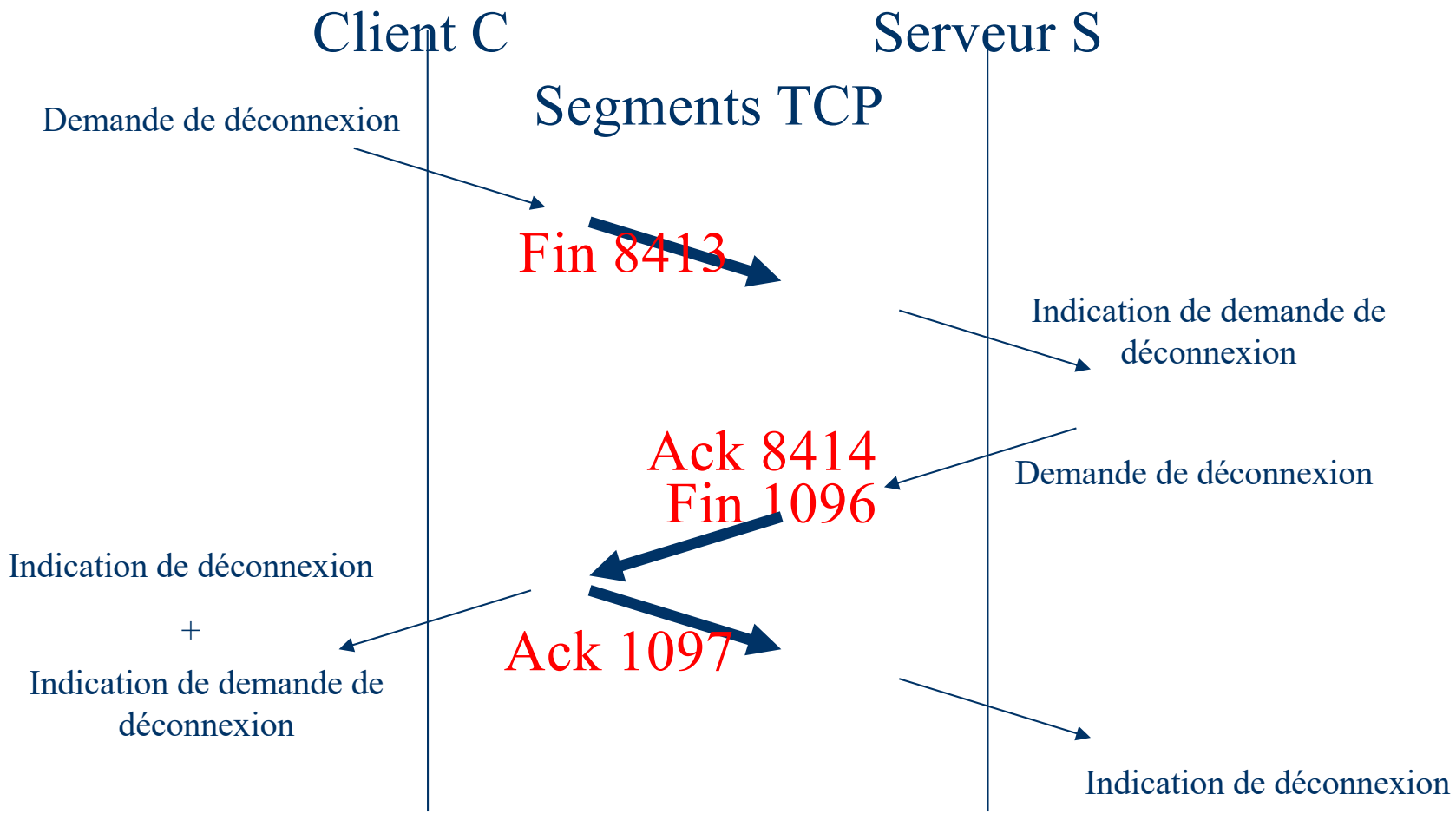
  Relâchement de cx = relâchement des 2 flots

  - L'entité initiatrice (généralement le client) envoie un segment de demande de relâchement de connexion
  - L'entité réceptrice (généralement le serveur) accepte en acquittant, et transmet une indication à l'application
  - L'entité « serveur », à la demande de l'application, envoie une segment de demande de relâchement de cx
  - L'entité « client », acquitte

Relâchement de connexion



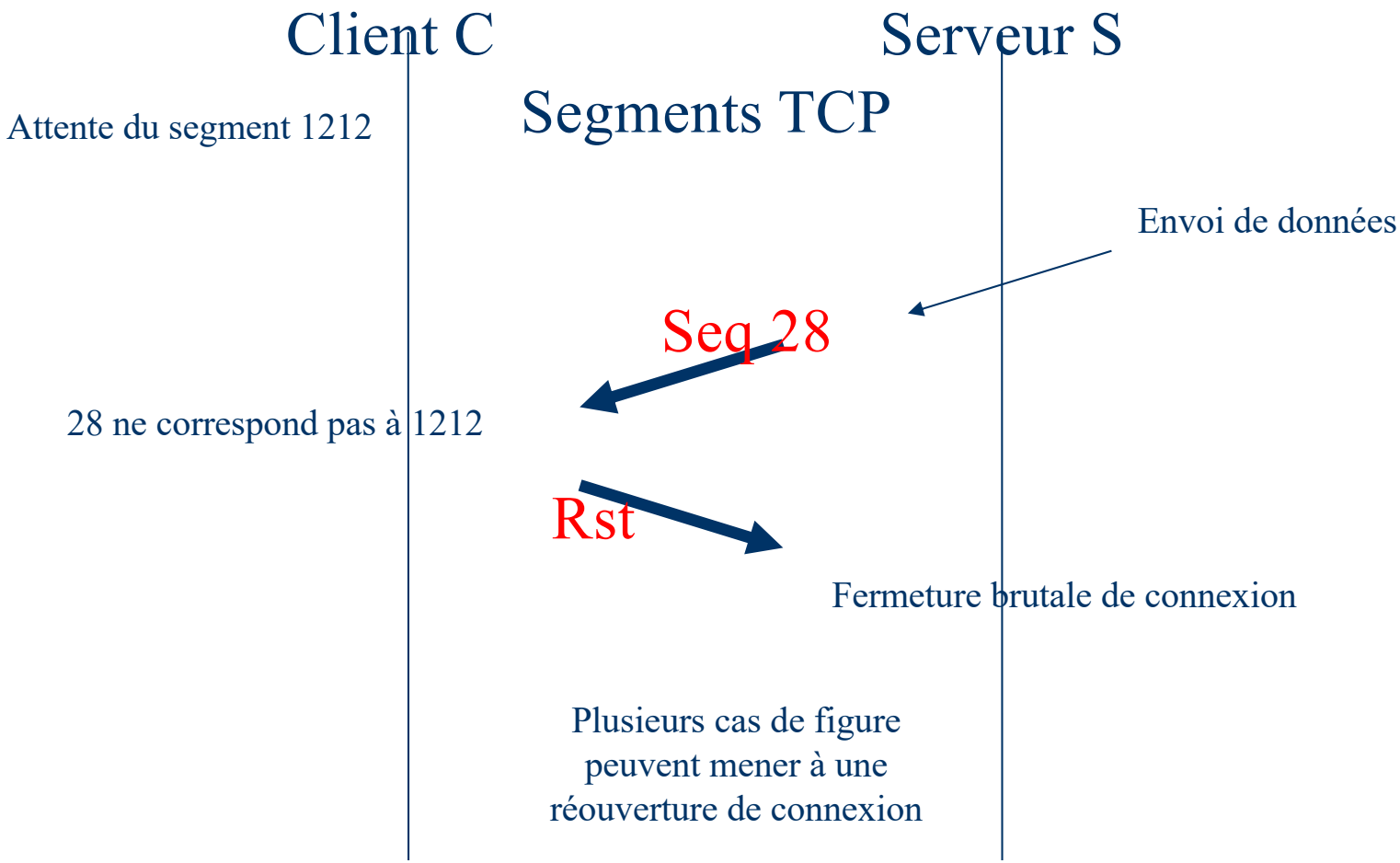
Relâchement de connexion



Réinitialisation de connexion

- Réinitialisation de connexion:
  - Intervient en cas de désynchronisation des deux extrémités ➔ détection d'anomalie
  - Une extrémité s'aperçoit d'une anomalie sur réception de données incohérentes (ex: numéro de séquence non attendu)

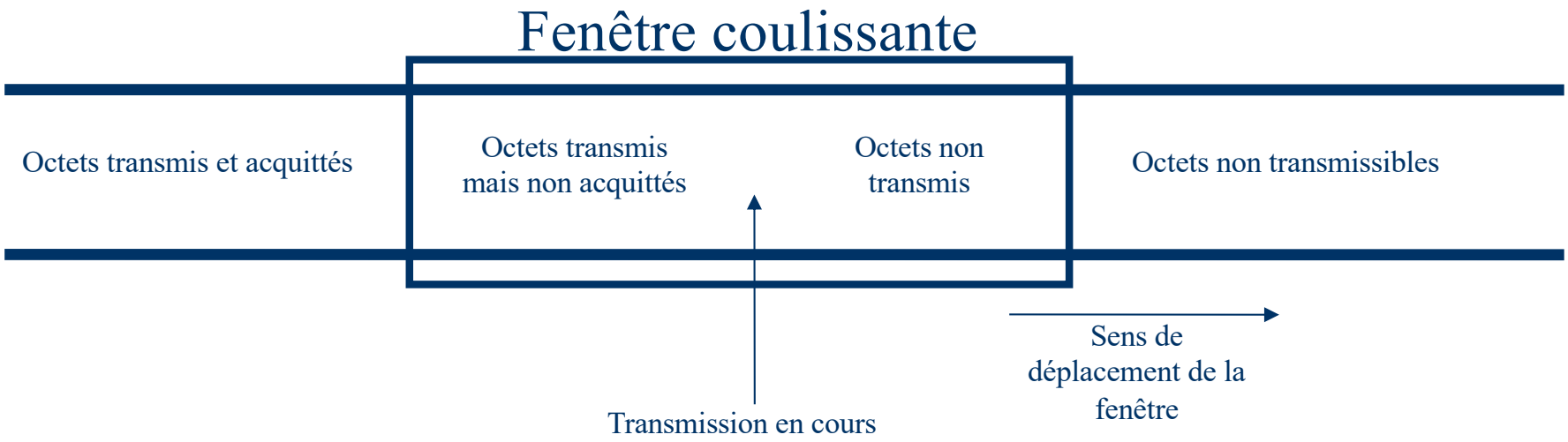
Réinitialisation de connexion



Contrôle de flux

- « Sliding Window » (fenêtre coulissante)
- ➔ l'émetteur peut continuer à émettre sans attendre tous les acquittements
- TCP opère au niveau de l'octet et non du segment
- ➔ on peut faire une reprise sur un numéro d'octet
- La largeur de la fenêtre définit le nombre d'octets maximal pouvant être émis sans être acquittés
- Chaque acquittement fait « glisser » la fenêtre de l'émetteur

Contrôle de flux



Contrôle de flux

- La taille de la fenêtre peut varier pendant la connexion

➔ le récepteur peut ainsi réguler le flux

- Remarque: Il n'existe pas de format différent pour les segments de données et les segments d'acquittement (idem HDLC). Ainsi, un transfert de données bi-directionnel peut être facilement mis en place.

Format d'un segment

<table>
<tr><td colspan="3">Port source</td><td>Port Destination</td></tr>
<tr><td colspan="4">Numéro de séquence</td></tr>
<tr><td colspan="4">Numéro d'acquittement</td></tr>
<tr><td>Lg ET</td><td>Réservé</td><td>Bits contrôle</td><td>Largeur fenêtre</td></tr>
<tr><td colspan="3">Checksum TCP</td><td>Pointeur d'Urgence</td></tr>
<tr><td colspan="4">Options TCP (+ Bourrage)</td></tr>
<tr><td colspan="4">Données</td></tr>
</table>

Format d'un segment

- Port source et destination (16 bits chacun)
  - Adresse des applications aux extrémités de la cx transport
- Numéro d'acquittement (32 bits)
  - Numéro du prochain octet de données attendu
- Numéro de séquence (32 bits)
  - Numéro du premier octet de données transmis sur le segment

Format d'un segment

- Longueur En-Tête (4 bits)
  - Longueur totale (partie fixe + options) de l'en-tête du segment TCP exprimée en multiple de 32 bits
- Largeur de fenêtre (16 bits)
  - Nb d'octets pouvant être émis sans acquittement
- Checksum TCP (16 bits)
  - Checksum calculé avec le pseudo en-tête
- Pointeur d'urgence (8 bits)
  - Position des données à traiter en priorité (cf contrôle)

Format d'un segment

- Bits de Contrôle (6 bits)

  URG ACK PSH RST SYN FIN

  - URG: le pointeur d'urgence doit être considéré
  - ACK: le numéro d'ack doit être considéré
  - PSH: transmission immédiate à la couche applicative (pas de tamponnement)
  - RST: fermeture de la connexion à cause d'une erreur irrécupérable (réinitialisation attendue)
  - SYN: Ouverture de connexion (premier segment)
  - FIN: demande de relâchement

Conclusion

- UDP n'apporte aucune plus value à IP (ou presque ...)
  - UDP matérialise le port
  - UDP calcule un checksum (+ pour IPv6)
  - MAIS…
  - Néanmoins très utile pour les services:
    - ne pouvant assumer de ré-émission (audio, vidéo,…)
    - dont les données tiennent dans un seul paquet, car:

➔ un paquet n'a pas de risque de déséquencement !

➔ un paquet dupliqué se voit tout de suite …

➔ la perte d'un paquet unique ne passe pas inaperçu !

Conclusion

- TCP apporte une énorme plus value à IP
  - TCP assure un service de réseau « parfait »
  - TCP matérialise le port
  - TCP calcule un checksum
  - MAIS …
  - Il est beaucoup plus lourd que UDP
  - ➔ phases de connexion et déconnexion nécessaires
  - Il n'est pas adapté aux réseaux à haut débit
  - Son digne successeur n'existe pas encore …
  - Quoi que … QUIC peut-être ?