Introduction aux réseaux (M212)

Abdulhalim Dandoush

Abdulhalim.dandoush@inria.fr

Office L143, Lagrange, INRIA

Slides de Joanna Moulierac

Déroulement du module

- 5 séances de cours de 1h les lundi de 8h à 9h
- 5 séances de TP de 4h

- **Contrôle continu :**
  - Contrôle sur les exercices faits en TPs

- **DS :**
  - Lundi 29 Juin du 14:30 a 15:30, salle 206LPCours

Bibliographie

Titre	Auteur	Année	Editeur
Initiation aux réseaux : cours et exercices	**Guy Pujolle**	**2000**	**Eyrolles**
Réseaux	**Guy Pujolle**	2005	Eyrolles
Réseaux - 4ème édition	Andrew Tanenbaum	2003	Pearson Education
Réseaux et Internet	**Douglas E. Comer**	08/2000	Campus Press

Outils utilisés à télécharger

- Simulateur réseau développé par CERTA
  - "© Réseau CERTA - Ministère de l'Éducation Nationale - www.reseaucerta.org"
  - http://archives.reseaucerta.org/outils/outils.php?num=236
  - Cisco Packet Tracer
  - https://www.netacad.com/group/offerings/packet-tracer
- Analyseur de trames réseaux : Wireshark
  - http://www.wireshark.org/

Plan du module

I. Introduction aux réseaux, classification des réseaux

II. Le modèle réseau en couches

III. **La couche liaison** : structures de trames, méthode de partage d'un medium CSMA/CD. Les réseaux locaux (LAN) : le standard Ethernet, VLAN

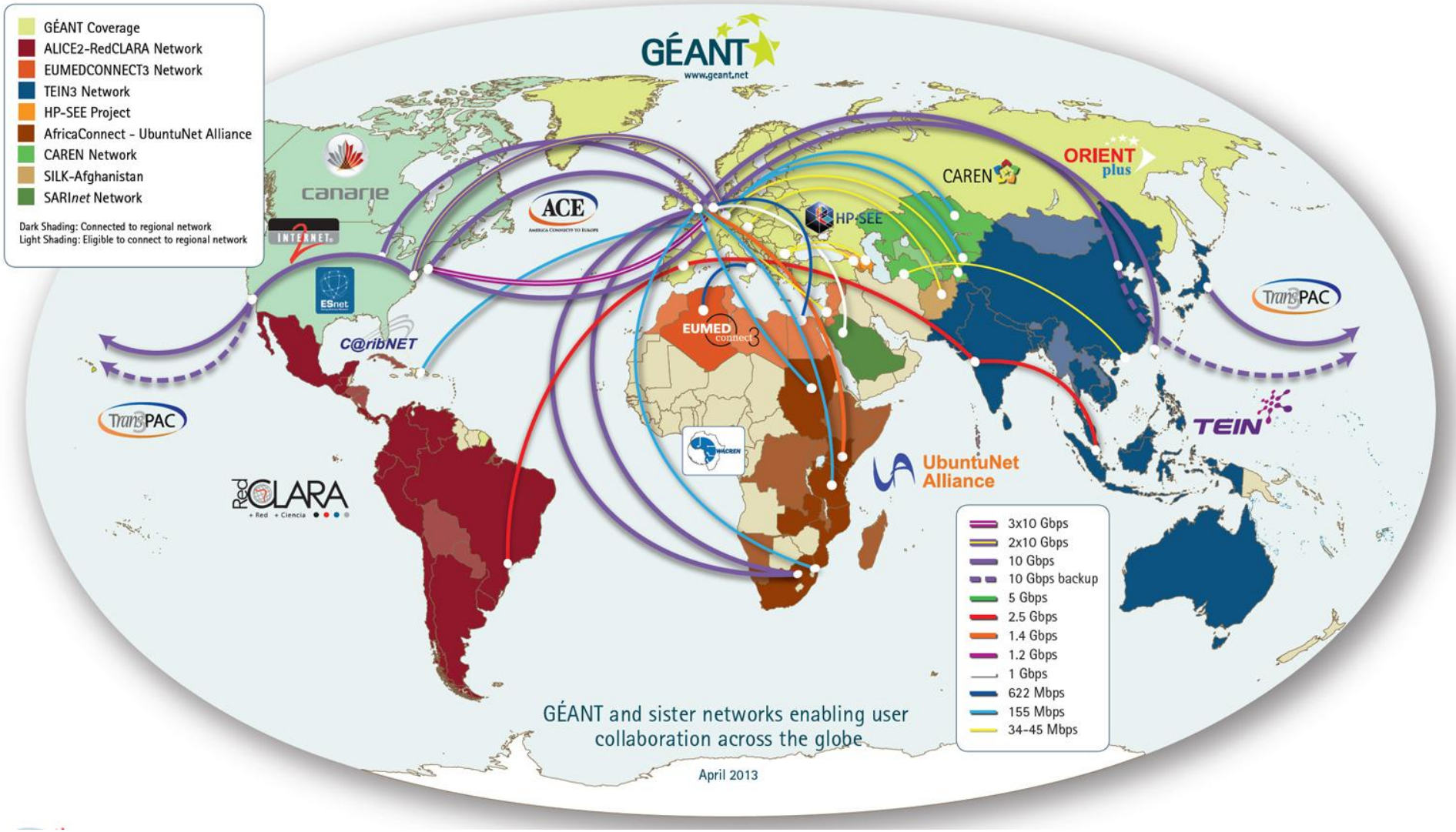
IV. **La couche réseau** : adressage IPv4, ARP, ICMP, routage IP…

Concept réseau

Définition : Un réseau est un ensemble **d'objets interconnectés** les uns avec les autres. Il permet de **faire circuler des éléments** entre chacun de ces objets selon des **règles bien définies**.

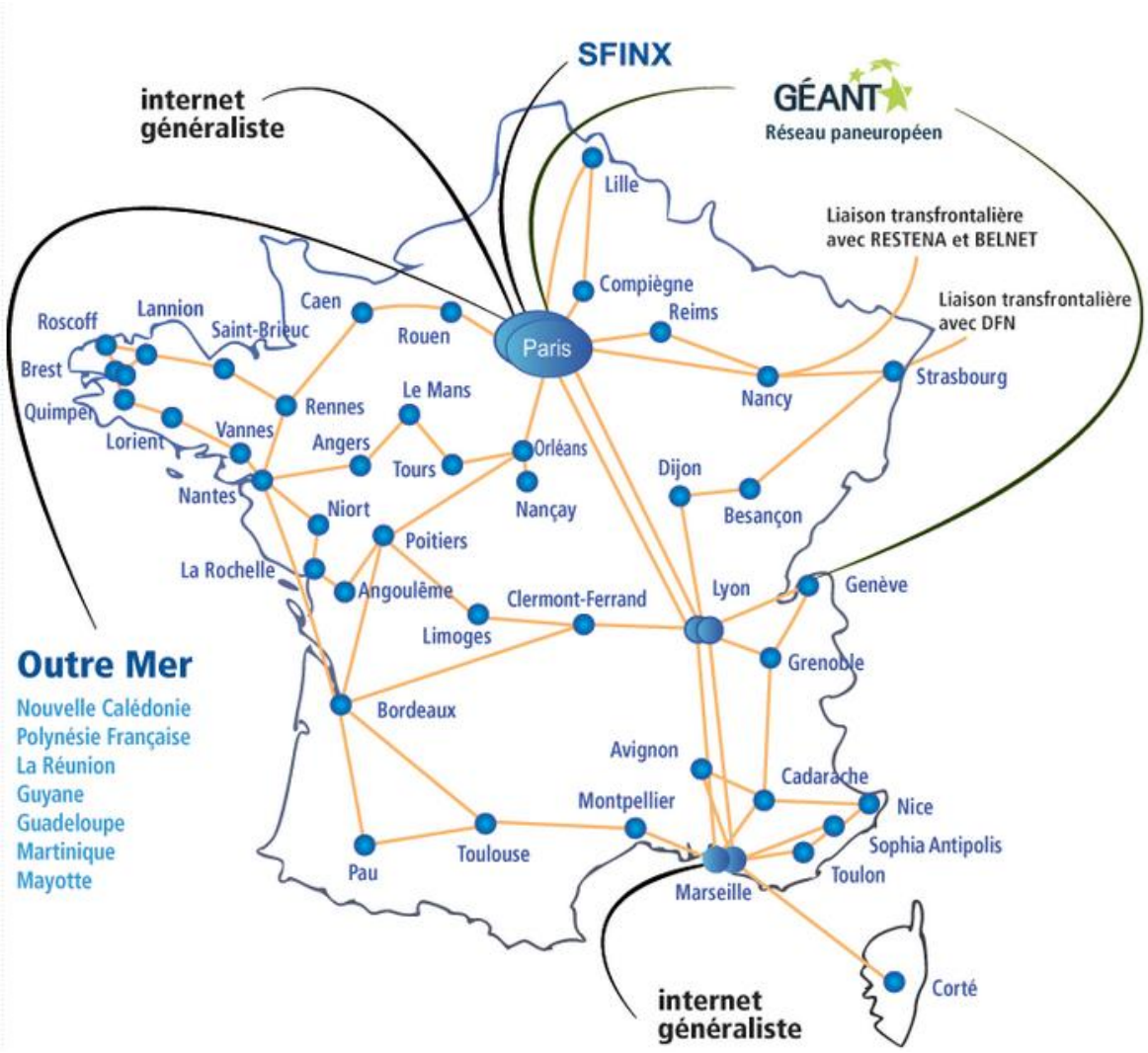
- réseau de transport
- réseau téléphonique
- réseau de distribution
- réseau de neurones
- réseau informatique

Le réseau Université/Recherche

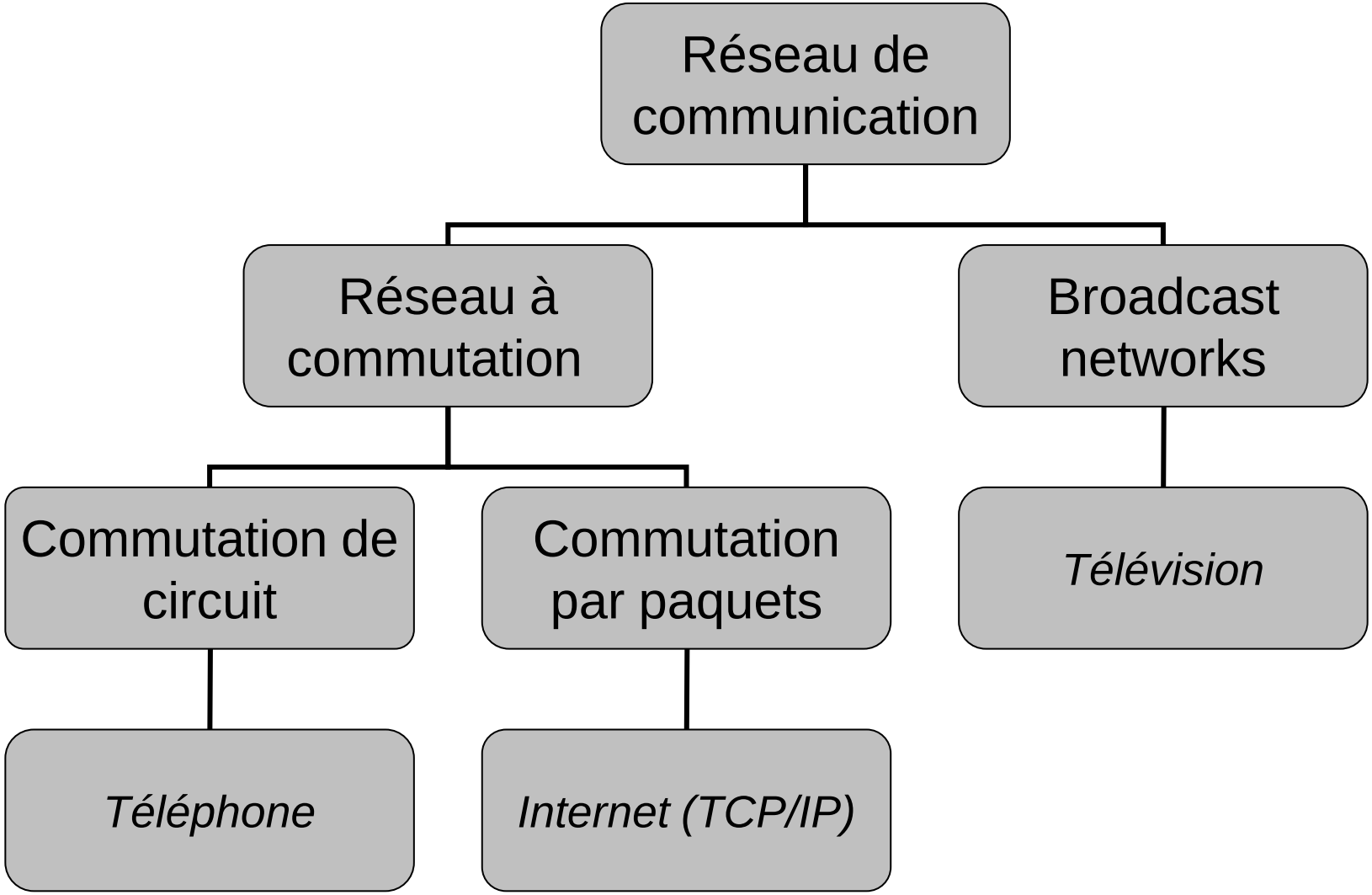


En France : Renater

- 11 900 km de fibres optiques,
- 72 points de présence (NR) (POP en En)
- Réseau : 125 longueurs d'onde 10G



Types de réseaux de communications



Objectifs et contraintes des réseaux

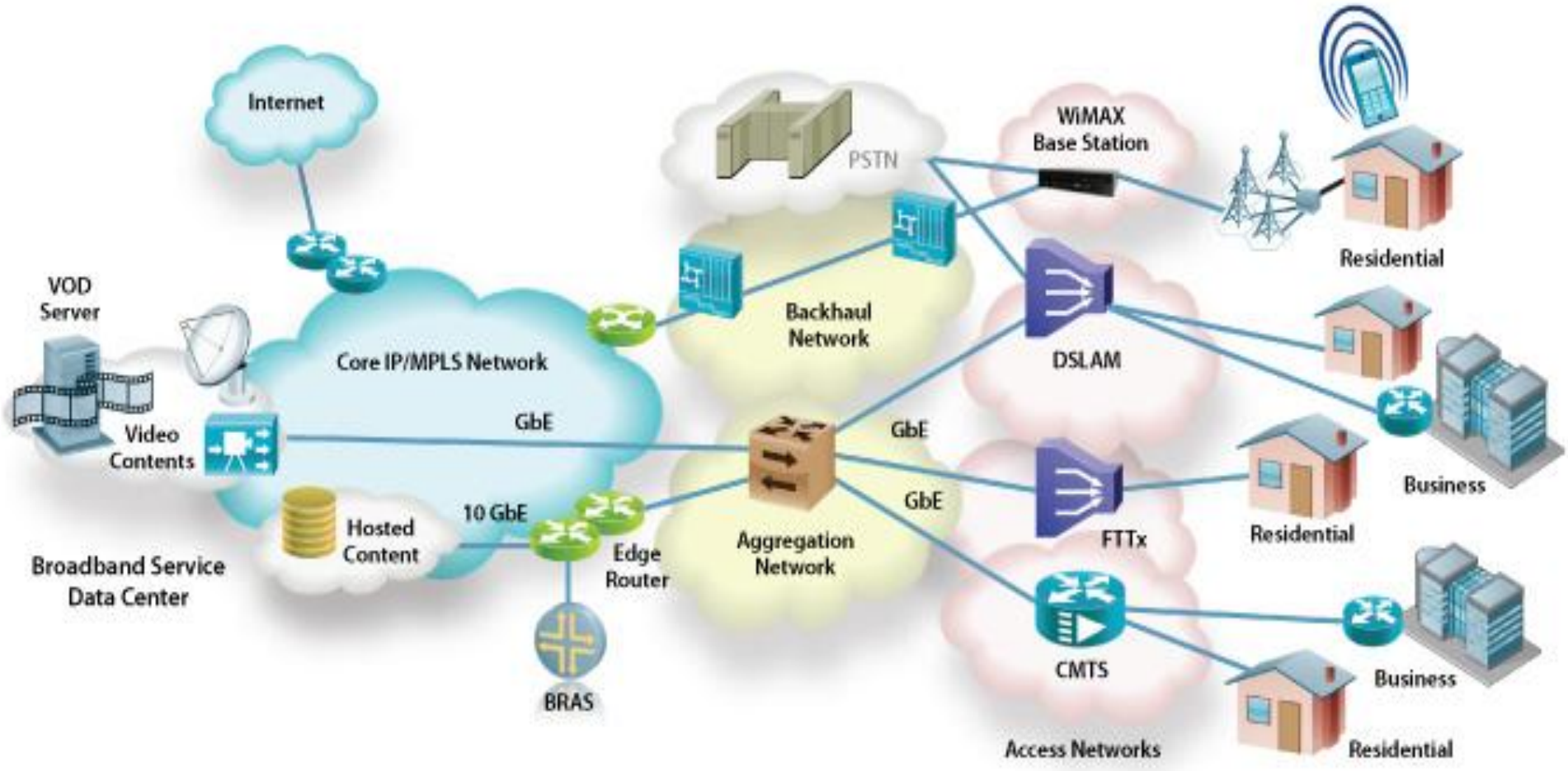
Les réseaux de télécommunications doivent assurer :

- la transparence géographique
- la transparence temporelle (vitesse de transmission)
- le partage de ressources
- l'accès à distance
- la communication inter application
- un certain niveau de qualité de service, de sécurité et de fiabilité

Diversité des réseaux

- Il n'existe pas un seul type de réseau
- Types d'ordinateurs différents, communiquant selon des **langages divers et variés**
- **Supports physiques** de transmission les reliant peuvent être très **hétérogènes :**
  - au niveau du transfert de données
    - circulation de données sous forme d'impulsions électriques,
    - sous forme de lumière, ou bien
    - sous forme d'ondes électromagnétiques
  - au niveau du type de support
    - lignes en cuivres,
    - Câble coaxiaux,
    - Fibre optiques,

Réseau hétérogène



Protocole de communications

- **Protocole** : ensemble des règles à suivre pour satisfaire des objectifs bien déterminés
- **Objectifs** : utiliser le canal de communication en évitant les collisions, le transfert fiable de données de bout en bout, etc.
- **Exemple de règles :**
  - le format des messages (nature des informations qu'il contient, leur emplacement dans le message)
  - le contrôle et l'envoi de données
  - les algorithmes de réaction à un évènement
  - Etc.

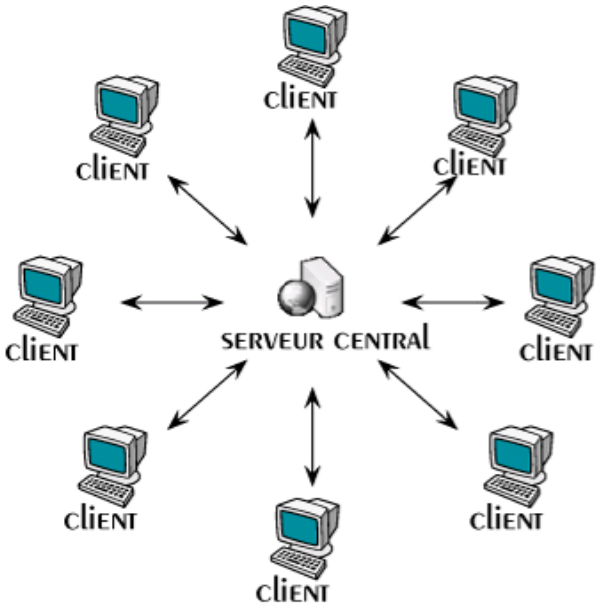
La normalisation

- Deux organismes de normalisation de droit s'occupent des réseaux informatiques
  - ISO (International Standardization Organization)
  - UIT-T (Union Internationale des Télécommunications)

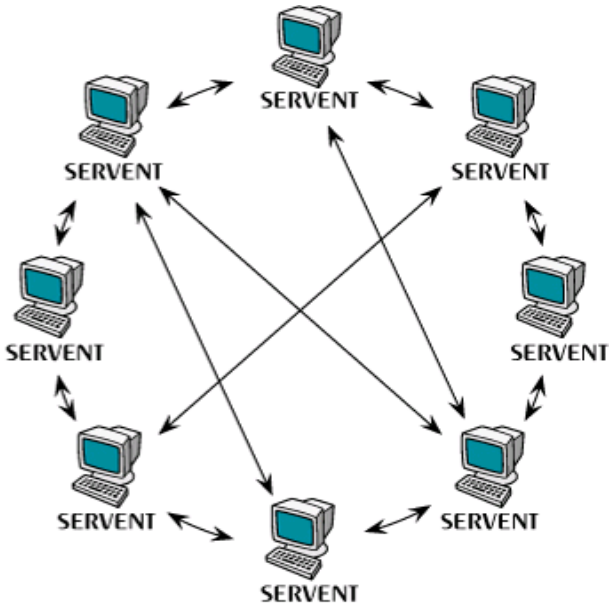
- La normalisation est menée par
  - ISOC (Internet Society)
  - IETF (Internet Engineering Task Force)

Deux types particuliers de réseaux

- Les réseaux pair à pair (peer to peer)
- Réseaux organisés autour de serveurs (Client/Serveur)



Architecture client-serveur



Architecture pair-à-pair

Pour assurer la communication, il faut…(1)

1. Adresser l'information au bon destinataire et lui indiquer l'identité de l'émetteur
2. Adopter une stratégie commune pour la représentation des données
3. Détecter les erreurs qui peuvent survenir lors de la transmission
4. Décomposer les messages trop longs en plusieurs morceaux

Pour assurer la communication, il faut…(2)

5. Assurer le réassemblage, chez le destinataire, d'un message décomposé
6. Détecter la perte de morceaux qui empêche le réassemblage
7. Coder l'information à transmettre pour l'adapter au support de transmission
8. Gérer les congestions du réseau

Importance de la standardisation

Peu de domaines ont autant besoin de standardisation

- Multiplicité des techniques réseaux
- La communication s'effectue entre systèmes hétérogènes
- Les équipements matériels et logiciels sont fournis par des constructeurs informatiques concurrents

Plusieurs standards sont apparus :

- **standards propriétaires réservés à un constructeur** : SNA d'IBM, NetWare de Novell, DECnet de Digital, ...
  - **standards ouverts de jure :** OSI de l'ISO, IEEE 802.*, X.25, ...
- **standards ouverts de facto :** TCP/IP, Ethernet, ...

II - Modèle de conception OSI

Le modèle OSI **(Open System Interconnection)** de l'ISO

- **But :** régler les problèmes d'interconnexion des systèmes hétérogènes (logiciel et matériel)

- **Principe** : Les fonctions remplies par un système de télécommunication sont segmentées en **couches superposées**
  - permettant de diviser l'ensemble des fonctions en modules,
  - possédant chacune une tâche bien définie.
  - chaque couche (excepté la couche la première) se sert des fonctions remplies par les couches inférieures pour remplir sa propre fonction

- Normalisé au début de 1980

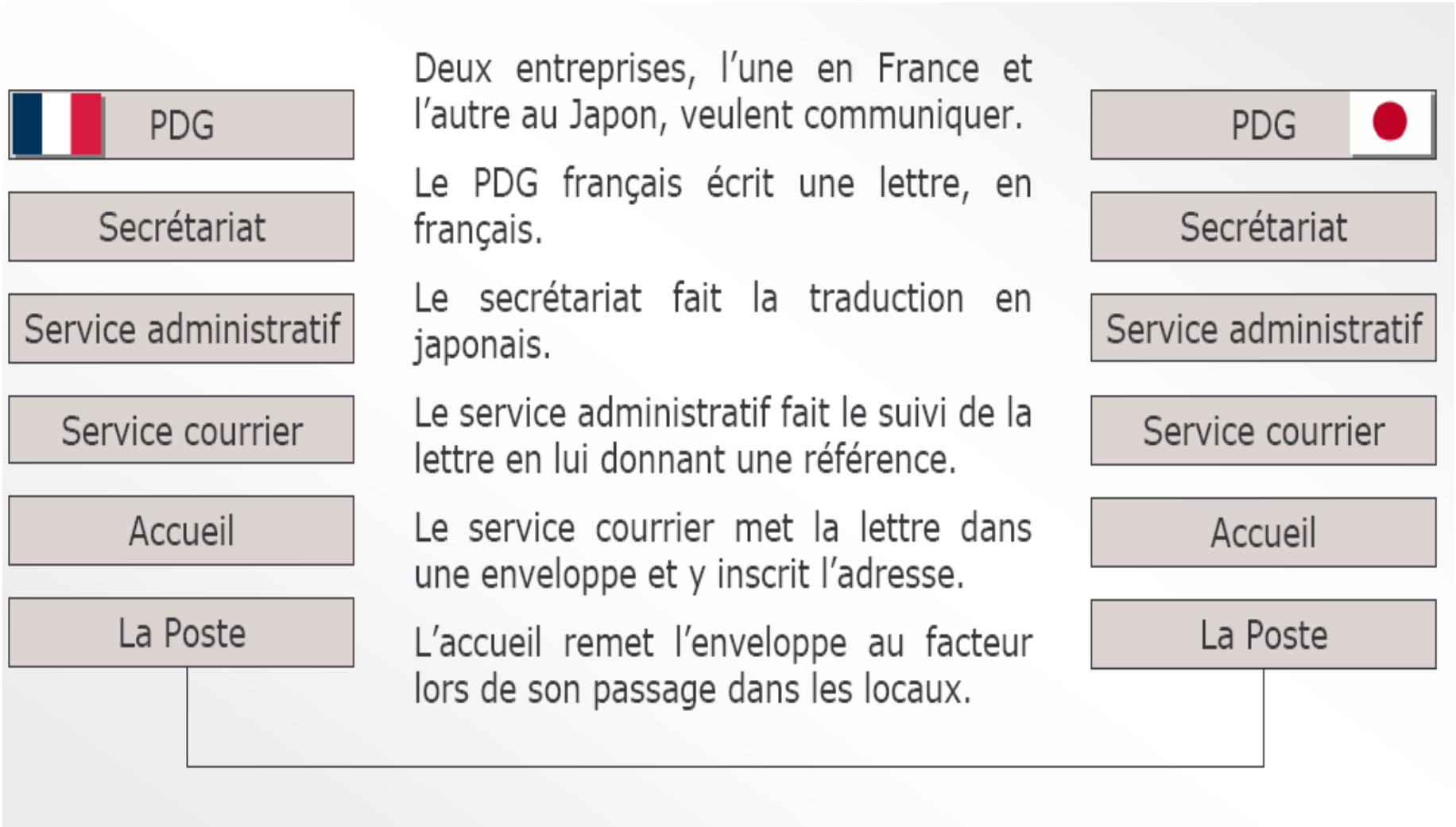
Conception du modèle OSI

- Découpage fonctionnel en **7 couches hiérarchiques** distinctes communicantes (entre couches adjacentes)
- Chaque couche a une fonction réseau spécifique et bien définie
- La structure en couche et la modularité facilitent la **maintenance et la mise à jour** des systèmes : la modification d'une couche reste transparente au reste du système
- On peut trouver plusieurs standards applicables pour une (ou plusieurs à la fois) couche OSI.

Pourquoi des couches ?

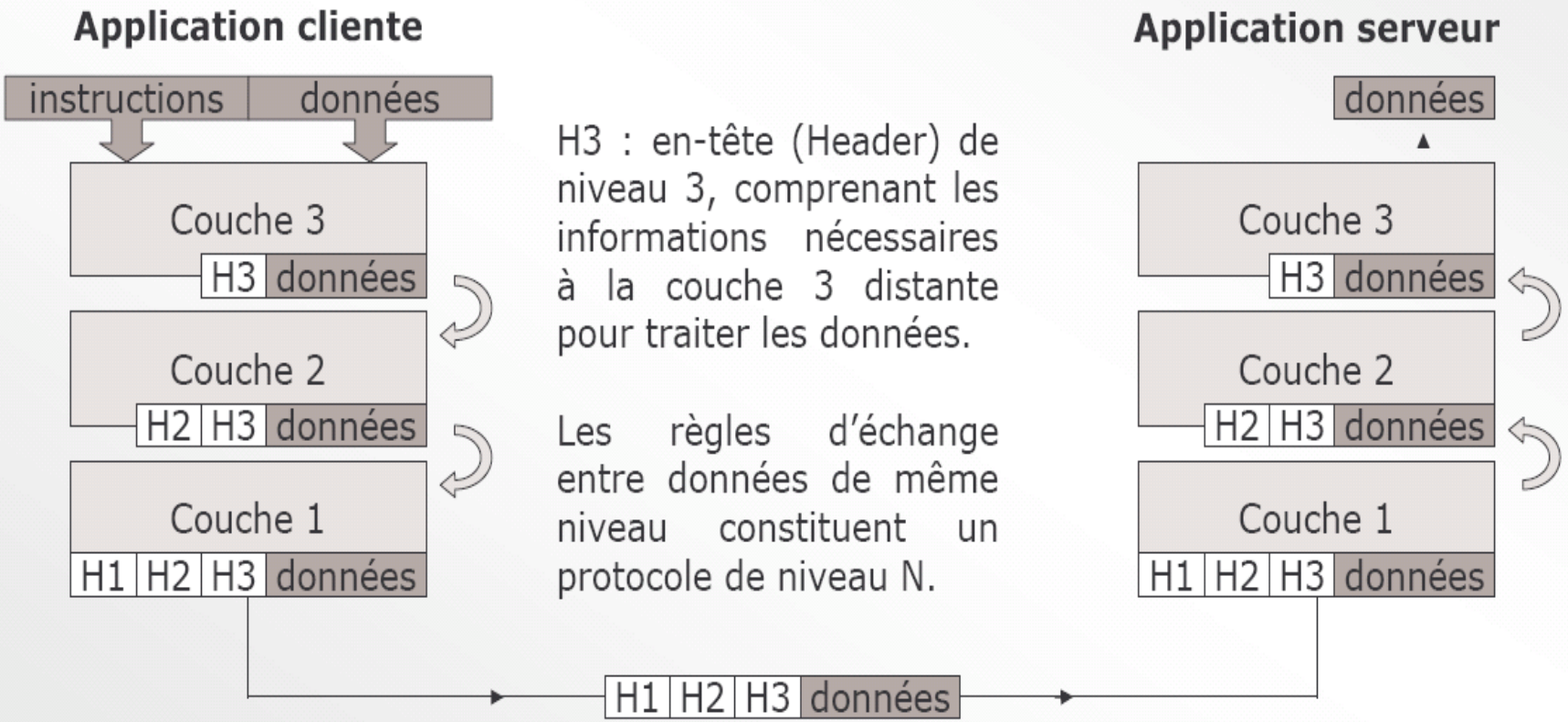
- Une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire,
- Chaque couche a des fonctions bien définies, les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles,
- Les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces,
- Le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes (homogénéité dans les fonctions de chaque couche) au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser,
- Restriction du nombre de couches fonctionnelles à une valeur raisonnable.

Analogie

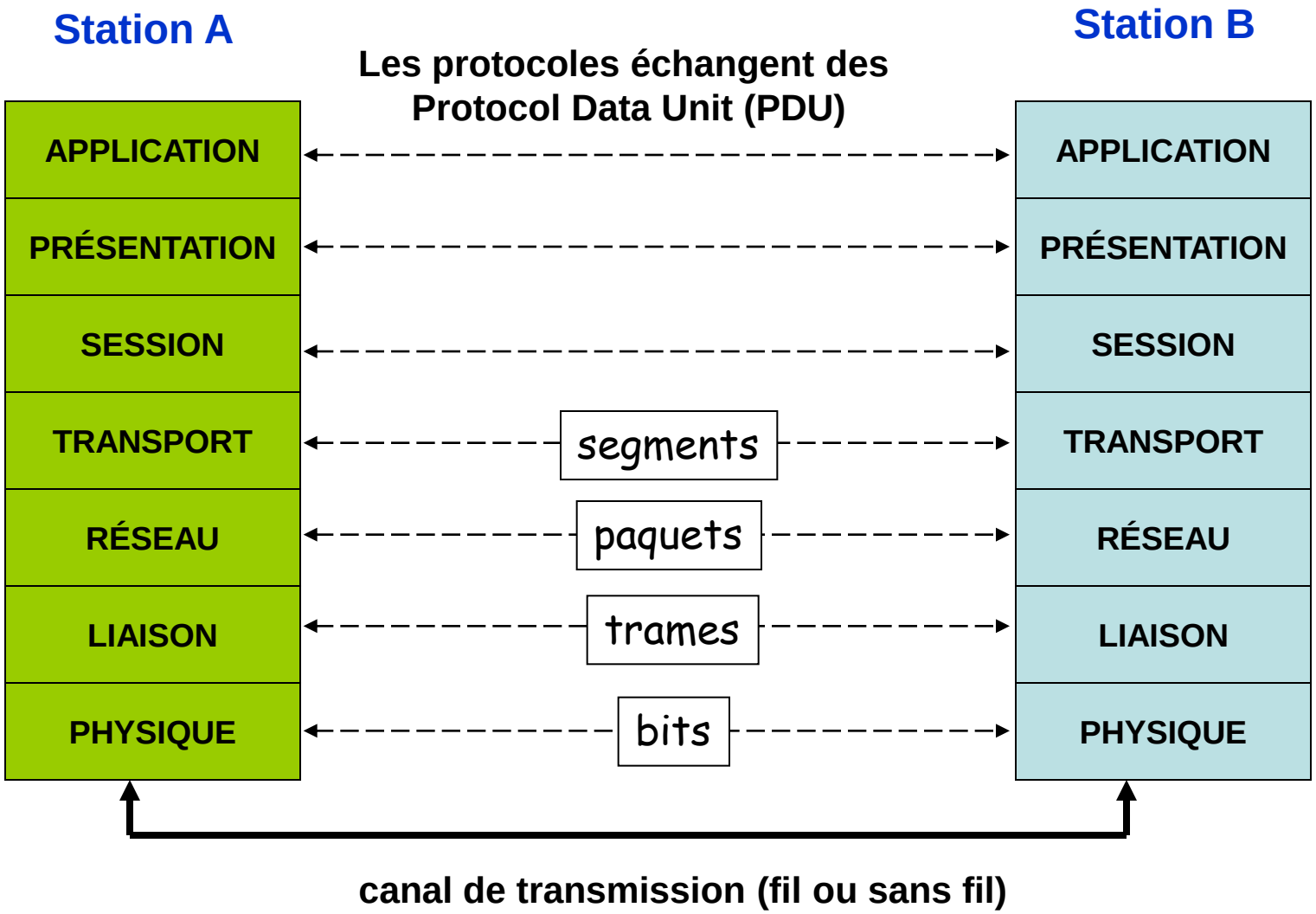

PDG
Secrétariat
Service administratif
Service courrier
Accueil
La Poste
Deux entreprises, l'une en France et l'autre au Japon, veulent communiquer.
Le PDG français écrit une lettre, en français.
Le secrétariat fait la traduction en japonais.
Le service administratif fait le suivi de la lettre en lui donnant une référence.
Le service courrier met la lettre dans une enveloppe et y inscrit l'adresse.
L'accueil remet l'enveloppe au facteur lors de son passage dans les locaux.
PDG
Secrétariat
Service administratif
Service courrier
Accueil
La Poste

Modèle simplifié à 3 couches

Exemple : modèle simplifié à trois couches



Les couches du modèle OSI



Les couches du modèle OSI

Deux moyens mnémotechniques pour se souvenir des 7 couches :

- **A**près **P**lusieurs **S**emaines **T**out **R**espire **L**a **P**aix
- **P**artout **L**e **R**oi **T**rouve **S**a **P**lace **A**ssise

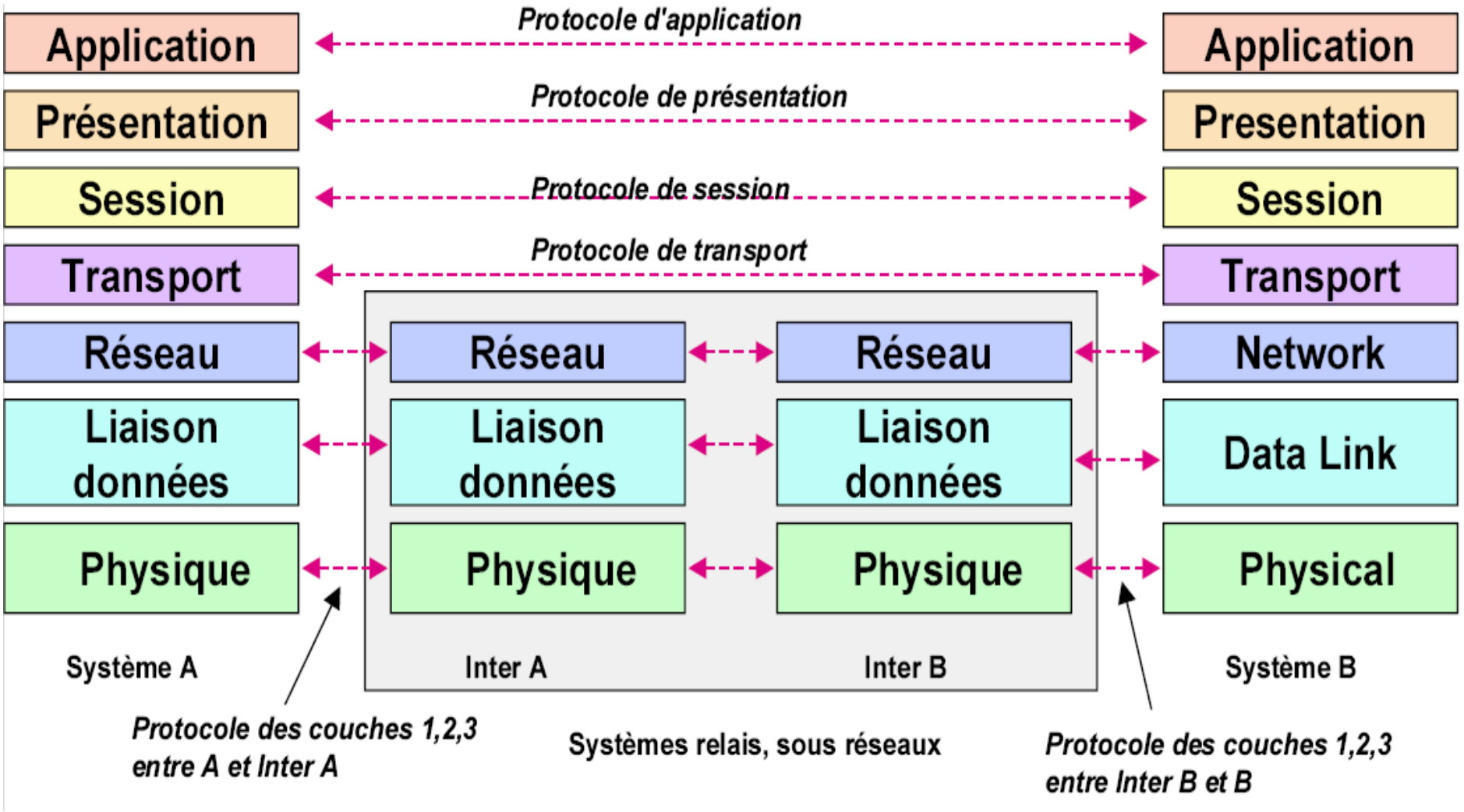
Fonctions des 7 couches

- **Couche 1** - **Physique** : transmet des bits de façon brute sur un support. Détermine la nature des signaux, la durée des bits, les connecteurs physiques.
- **Couche 2** – **Liaison** : transfert de l'information sous forme de trames, détection et correction d 'erreurs, échange entre nœuds voisins. *Adressage physique des noeuds*.
- **Couche 3** – **Réseau** : achemine des paquets de bout à bout : routage à travers les réseaux et nœuds intermédiaires. *Adressage logique* des *nœuds.*

Fonctions des 7 couches

- **Couche 4** – **Transport** : assure le transport de l'information de bout en bout de la connexion, procédure de connexion et déconnexion. Contrôle le flux.
- **Couche 5** – **Session** : organise l'échange de données et structure le dialogue entre les applications.
- **Couche 6** – **Présentation** : gère les différences de syntaxe de l'information (alphabet, présentation de graphiques etc.). Offre des mécanismes de sécurité d 'accès à l 'information, de cryptage, de compression.
- **Couche 7** – **Application** : protocoles applicatifs pour le dialogue entre applications. Les applications accèdent aux services réseaux par les services de cette couche.

Systeme terminal vs. intermédiaire



Fonctionnement du modèle

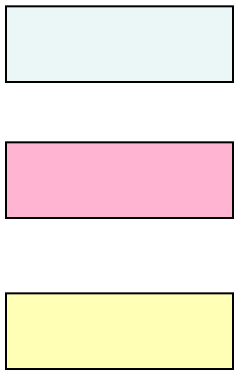
- Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice.
- A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un **en-tête**, ensemble d'informations qui garantit la transmission.
- Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel...

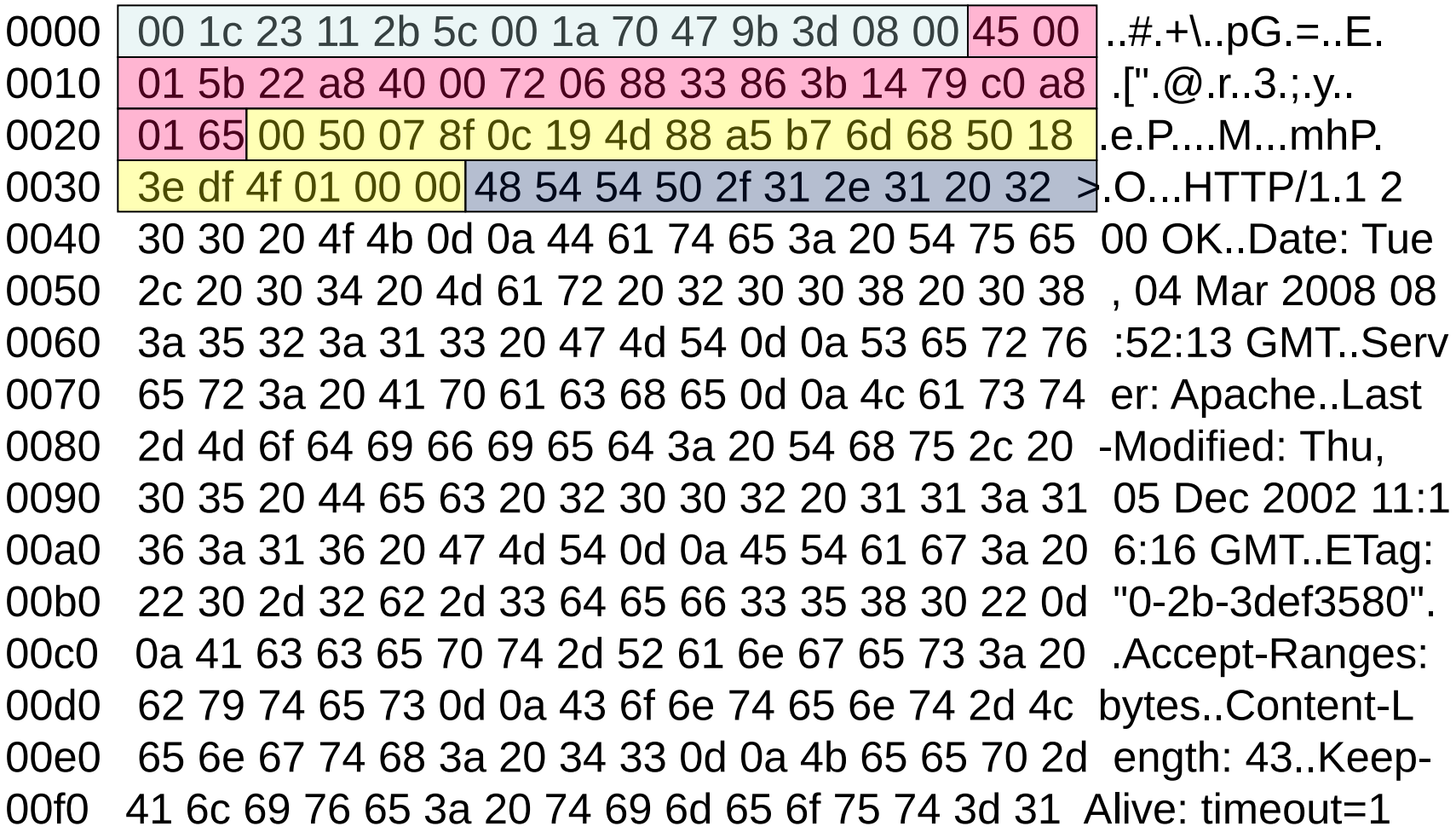
Fonctionnement du modèle

- Chaque couche est programmée comme si elle était vraiment horizontale, c'est à dire qu'elle **dialoguait directement avec sa couche paire réceptrice**.
- A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :
  - **Physique** : bit
  - **Liaison** : trames
  - **Réseau** : paquets
  - **Transport** : messages

Ce qui circule sur Internet :

```
0000  00 04 de 1f 78 0a 00 1c  23 11 2b 5c 08 00 45 00   ....x... #.+\..E.
0010  00 28 a9 d7 40 00 80 06  b5 cd 8a 60 f1 58 48 0e   .(..@... ...`.XH.
0020  d7 63 05 3e 00 50 92 43  82 a4 cd e5 8b f2 50 10   .c.>.P.C ......P.
0030  fb 5e a4 fc 00 00                                 .^....
```




0000 00 1c 23 11 2b 5c 00 1a 70 47 9b 3d 08 00 45 00 ..#.+\..pG.=..E.
0010 01 5b 22 a8 40 00 72 06 88 33 86 3b 14 79 c0 a8 .["·@·r··3·;·y··
0020 01 65 00 50 07 8f 0c 19 4d 88 a5 b7 6d 68 50 18 .e·P····M···mhP·
0030 3e df 4f 01 00 00 48 54 54 50 2f 31 2e 31 20 32 >·O···HTTP/1·1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK··Date: Tue
0050 2c 20 30 34 20 4d 61 72 20 32 30 30 38 20 30 38 , 04 Mar 2008 08
0060 3a 35 32 3a 31 33 20 47 4d 54 0d 0a 53 65 72 76 :52:13 GMT··Serv
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 4c 61 73 74 er: Apache··Last
0080 2d 4d 6f 64 69 66 69 65 64 3a 20 54 68 75 2c 20 -Modified: Thu,
0090 30 35 20 44 65 63 20 32 30 30 32 20 31 31 3a 31 05 Dec 2002 11:1
00a0 36 3a 31 36 20 47 4d 54 0d 0a 45 54 61 67 3a 20 6:16 GMT··ETag:
00b0 22 30 2d 32 62 2d 33 64 65 66 33 35 38 30 22 0d "0-2b-3def3580"·
00c0 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 ·Accept-Ranges:
00d0 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes··Content-L
00e0 65 6e 67 74 68 3a 20 34 33 0d 0a 4b 65 65 70 2d ength: 43··Keep-
00f0 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 Alive: timeout=1

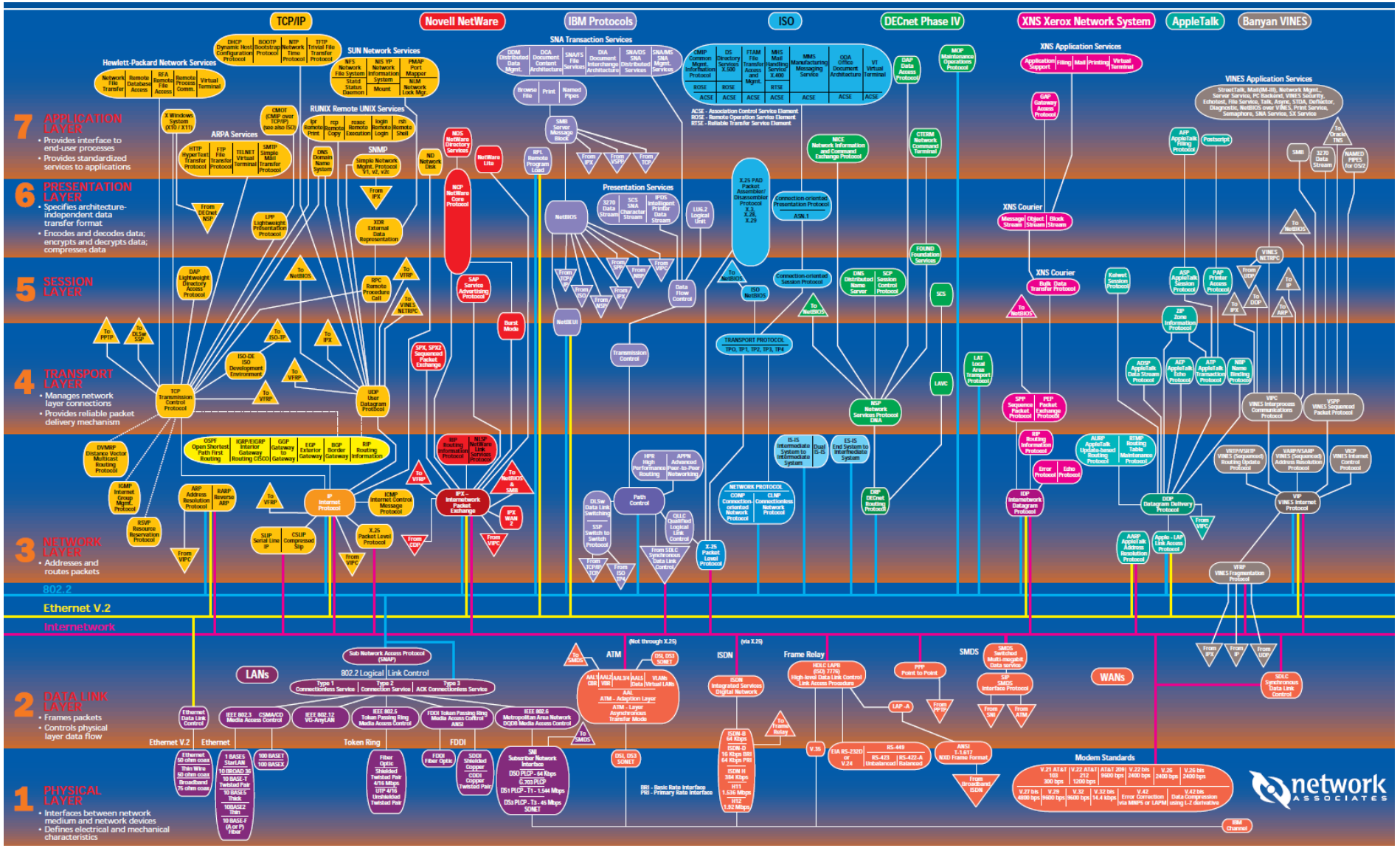
Commentaires sur le modèle OSI

- Le modèle OSI est juste un **modèle de référence**
- Il n'est pas nécessaire que les systèmes soient implantés suivant la description du modèle de référence
- Le système n'est pas forcément organisé en 7 modules ou tâches assurant chacune les fonctions de l'une des 7 couches !
  - **Exemple :** le modèle TCP/IP est constitué de 5 couches
- Une couche peut exister et être vide car une couche peut regrouper un ensemble de fonctions qui ne sont pas mises en oeuvre !
- Dans ce dernier cas, soit le service n'est pas nécessaire à la couche supérieure, soit il est déjà rendu par la couche inférieure

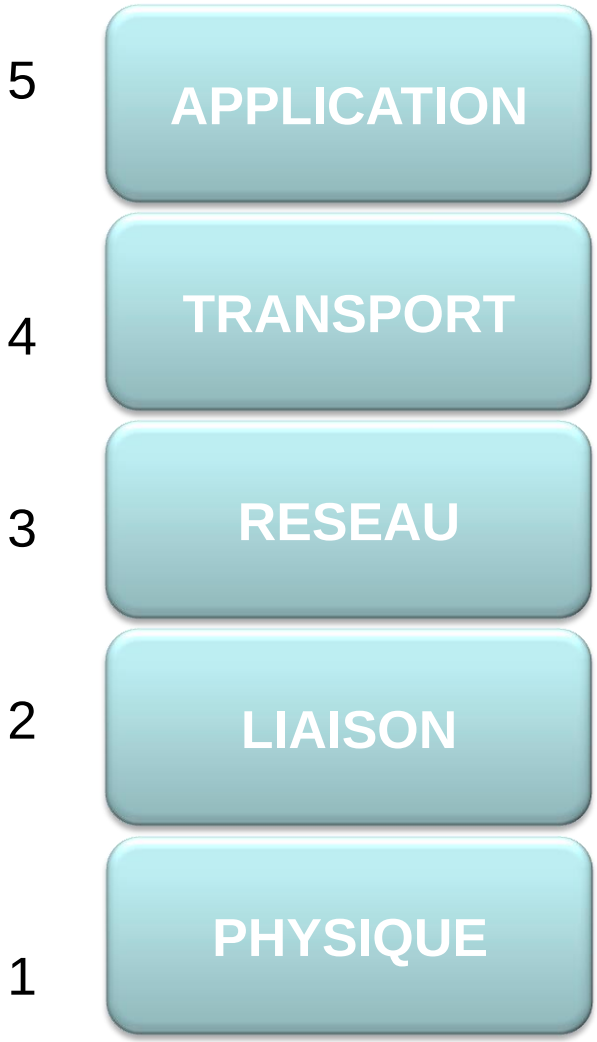
Critique du modèle OSI

- Structure réseau la plus étudiée et la plus unanimement reconnue et pourtant ce n'est pas le modèle qui a su s'imposer !
- **Pas le bon moment** : lorsque le modèle OSI est sorti, les universités américaines utilisaient déjà largement TCP/IP et les industriels n'ont pas ressenti le besoin d'investir dessus.
- **Trop complet et trop complexe** : peu de programmes peuvent utiliser ou utilisent mal l'ensemble des 7 couches du modèle, les couches session et présentation sont fort peu utilisées et à l'inverse les couches liaison de données et réseau sont très souvent découpées en sous-couches tant elles sont complexes.

Les protocoles réseaux



Modèle hybride finalement utilisé



	Protocoles étudiés en cours	Equipements
5 APPLICATION	HTTP – FTP – SMTP – POP – IMAP – TELNET	
4 TRANSPORT	TCP – UDP	
3 RESEAU	IP (v4 ou v6) - ICMP – ARP @IP	ROUTEUR
2 LIAISON	ETHERNET – WIFI – CSMA/CD et CSMA/CA – VLAN - @mac	SWITCH
1 PHYSIQUE		HUB

La couche physique

- La couche physique est chargée de la transmission des signaux électriques ou optiques entre les interlocuteurs.
- Emission et la réception d'un bit ou d'un train de bits continu.
- Elle transmet un flot de bits sans en connaître la signification ou la structure.
- Elle code l'information pour l'adapter au support de transmission et effectue la conversion entre bits et signaux électriques, électromagnétiques ou optiques.
- Elle normalise les signaux envoyés sur le support (analogique / numérique, voltage, optique etc…) ainsi que le type et la longueur des câbles, les connecteurs utilisés…

Supports physiques de transmissions

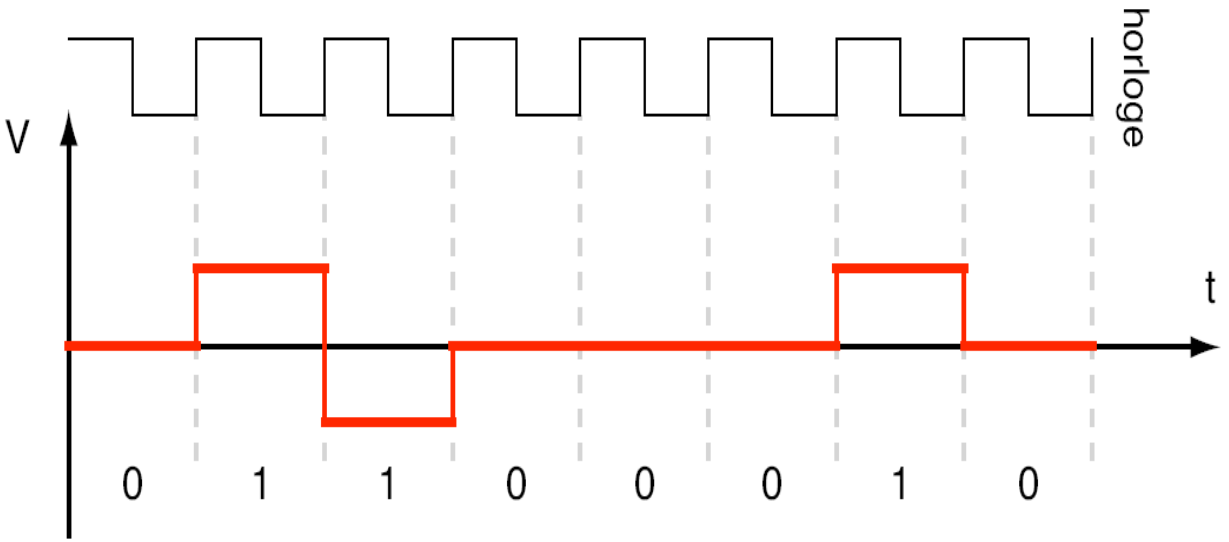
- Circulation des informations entre les équipements de transmission.

- Trois catégories principales, selon le type de grandeur physique qu'ils permettent de faire circuler :
  - **Les supports filaires** permettent de faire circuler une grandeur électrique sur un câble généralement métallique
  - **Les supports aériens** désignent l'air ou le vide, ils permettent la circulation d'ondes électromagnétiques ou radioélectriques diverses
  - **Les supports optiques** permettent d'acheminer des informations sous forme lumineuse

Code Bipolaire

Code tout ou rien dans lequel :

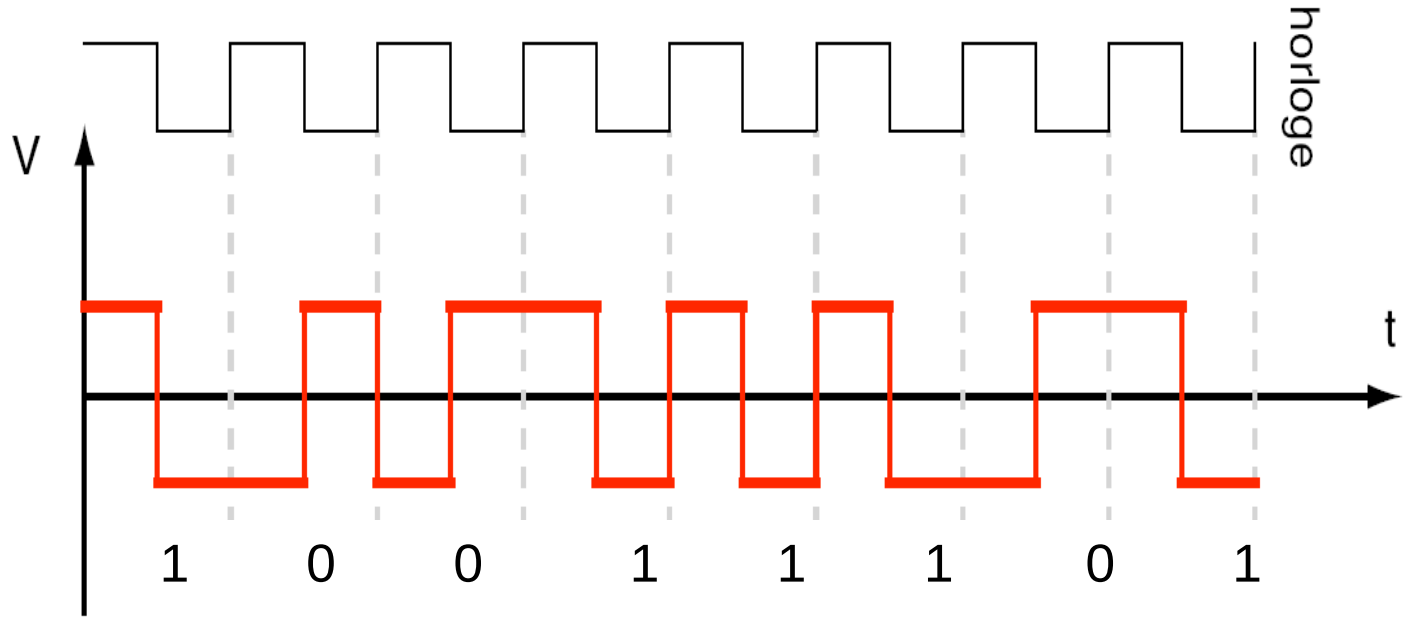
- le « 0 » est représenté par une tension nulle;
- le « 1 » est représenté par une tension alternativement positive ou négative pour éviter de maintenir des tensions continues.



- Avantage : indépendant de la polarité
- Problèmes de désynchronisation et de détection de transmission

Code Biphase ou Manchester

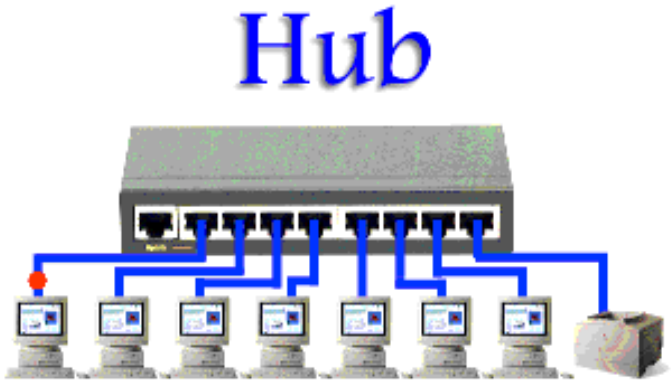
Le signal change au milieu de l'intervalle de temps associé à chaque bit. Au milieu de l'intervalle il y a une transition de bas en haut pour un « 0 » (front montant) et de haut en bas pour un « 1 » (front descendant).



- **Principe :** XOR entre les données et l'horloge
- Codage utilisé pour Ethernet à 10 Mbit/s

Hub (concentrateur)

- Equipement au niveau physique
  Reçoit les trames (paquets de la couche liaison) d'un port et les diffusent (broadcast) sur toutes ses sorties
- Mauvais du point de vue sécurité
- Cet équipement est équivalent au répéteur multiport
- Obsolète



III - Couche Liaison : Ethernet

Couche liaison

- Découpage des données en trames.
- Donne une signification aux bits qui sont transmis sur le réseau
- Elle doit acheminer sans erreur des blocs d'information utilisateur sur la liaison physique :
  - **Contrôle d'intégrité :** détection et de correction d'erreurs élémentaires dues au support physique imparfait et signale à la couche réseau les erreurs irrécupérables.
- Reconnaissance des débuts et fin de trames réceptionnées.
- Spécifications des tailles et moyens d'adressage des paquets.
- Elle s'assure que deux ou plusieurs nœuds n'essaient pas de transmettre des données sur le canal (partagé) de transmission en même temps.

- **Exemples :**
  - HDLC (High Data Link Protocol), PPP (Point to Point Protocol), Ethernet (IEEE 802.3).

Réseaux locaux / Local Area Network

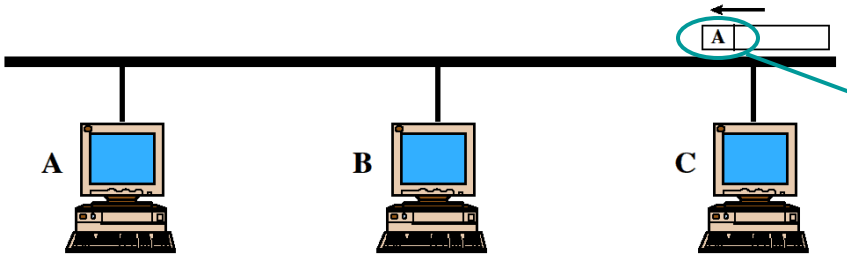
- Support de transmission partagé par plusieurs équipements (en général) : **réseau à diffusion**.
- Un nœud peut vouloir envoyer à une, plusieurs ou tous les nœuds
- Un nœud peut vouloir émettre à tout moment
- Si support partagé, alors il faut :
  - Une manière d'identifier chaque nœud : des adresses (au niveau de la couche Liaison)
  - Des règles pour gérer le « droit de parole » : méthodes d'accès au support

Les réseaux Ethernet

- Technologie de réseau local permettant que toutes les machines d'un réseau soient connectées à une même ligne de communication, formée de câbles cylindriques (câble coaxial, paires torsadées)
- Rapidement, dû à leur popularité, les réseaux Ethernet (et plus généralement les réseaux locaux) ont donné naissance à des normes spécifiques.
- Dans le cas d’un réseau Ethernet, ces normes sont les IEEE 802.2 et IEEE 802.3

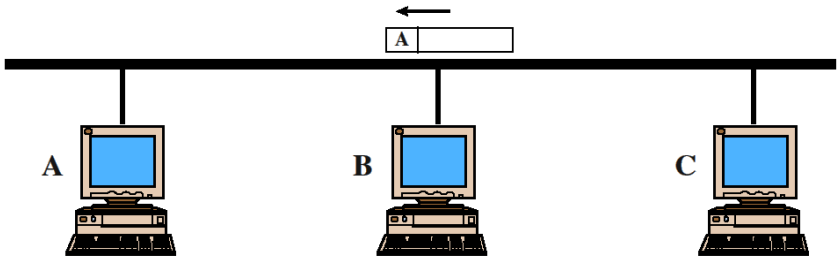
Illustration d'un support partagé

C émet une trame destinée à A

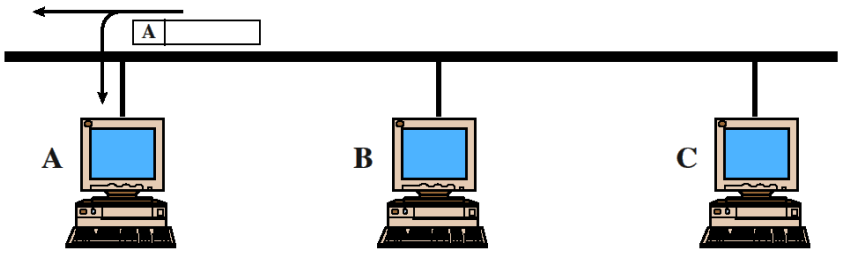


Adresse du destinataire

La trame n'est pas destinée à B
⇒ B l'ignore



A lit la trame au passage de celle-ci



Dessins : [Stallings, 2002]

Histoire d'Ethernet

- Sur la base du projet ALOHA conçu pour effectuer des communications radio entre des **machines éparpillées** sur les îles Hawaï en 1970
- Ethernet expérimental à 3 Mbit/s (Xerox, 1973)
- Ethernet à 10 Mbit/s (Digital, Intel et Xerox, 1982)
- Normalisation IEEE 802.3 en 1985

Evolution du câblage : câble coaxial à l'origine, puis paire torsadée, et fibre optique

Evolution des appareils : répéteurs, ponts, concentrateurs, commutateurs..

- Ethernet s'impose face à d'autres standards comme le Token Ring

Evolution des vitesses : 10 Mbits/s, 100 Mbits/s, 1 Gbits/s, 10 Gbits/s…

Normalisation IEEE 802

Comité pour la normalisation des réseaux locaux (LAN) et métropolitains (MAN)

Normalise les couches 1 et 2 du modèle OSI

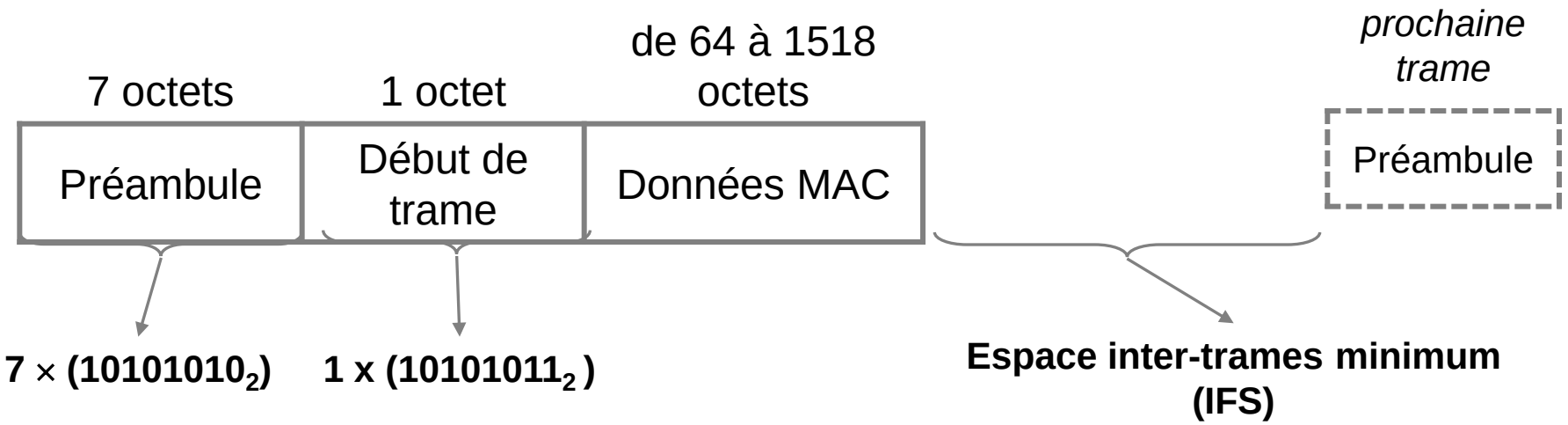
- Quelques sous-groupes et normes IEEE 802
  - 802.3 : topologie en bus
  - 802.5 : anneau à jeton (token ring)
  - 802.4 : bus à jeton (token bus)

  } **réseaux câblés**

  - 802.11 : réseaux locaux sans fil (wireless LAN)

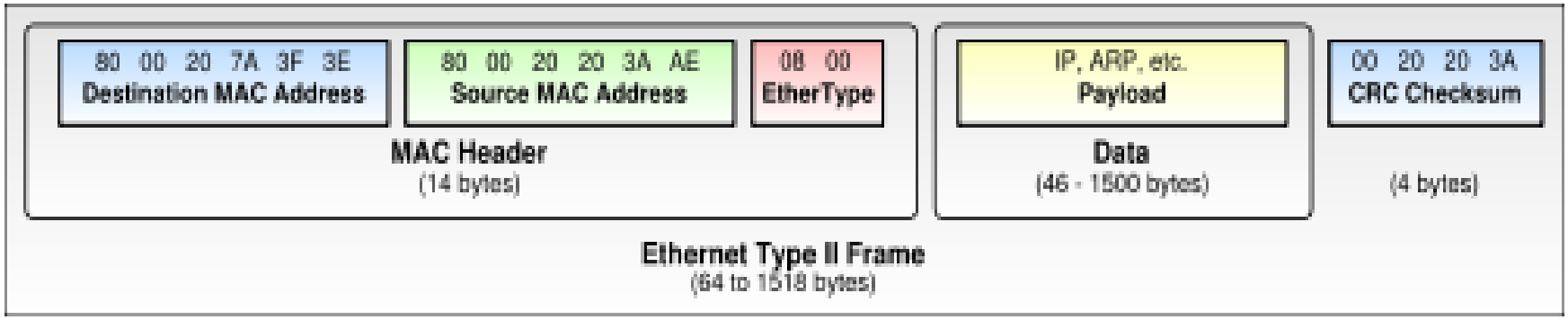
Encapsulation des trames Ethernet et 802.3 au niveau physique

Les trames sont précédées d'un préambule et suivies d'un temps de repos



- Préambule : permet la synchronisation du récepteur (10101010$_2$ = signal carré, en codage Manchester)
- Espace inter-trames : permet de bien séparer les trames successives
  ⇨ **802.3 / Ethernet à 10 Mbit/s : IFS = 9,6 µs**

Structure d'une trame éthernet



- Adresse MAC destination : 6 octets
- Adresse MAC source : 6 octets
- Type : 2 octets
  - Indique le protocole situé sur la couche de niveau supérieur

Ethernet : valeur du champ type

Champ Type (hexadécimal)	Protocole couche supérieure (encapsulé dans la trame)
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x86DD	IPv6
0x8864	PPPoE

source : http://www.iana.org

Caractéristiques d'un réseau éthernet

- Norme **IEEE 802.3**
- Topologie en **bus linéaire** ou en **bus en étoile**
- Transmission des signaux en **bande de base**
- Méthode d'accès au réseau **CSMA/CD**, méthode à contention
- Le support est « **passif** » (c'est l'alimentation des ordinateurs allumés qui fournit l'énergie au support) ou « **actif** » (des concentrateurs régénèrent le signal)
- Le câblage en **coaxial**, en **paires torsadées** et en **fibres optiques**
- Les connecteurs **BNC, RJ45**, **AUI** et/ou les connecteurs pour la fibre optique
- Des trames de **64 à 1518 Octets**

Taille des trames ethernet / IEEE 802.3

- Taille maximale = 1518 octets
  - Empêche une station de monopoliser le canal pendant trop longtemps
  - Valeur arbitraire
- Taille minimale = 64 octets
  - Détection des collisions
    - 64 octets (MAC, CRC inclus) + 8 octets (en-tête trame physique - préambule) = 72 octets au total sur la ligne = plus petite trame correcte
  - Si la quantité de données transportées ne permet pas de remplir une trame, il faut ajouter des octets de bourrage (padding)

Les adresses MAC

- Les LANs de type Ethernet et 802.3 sont des réseaux dits de broadcast (diffusion), ce qui signifie que tous les hôtes voient toutes les trames.

- L’adressage MAC est donc un élément important afin de pouvoir déterminer les émetteurs et les destinataires en lisant les trames.

Les adresses MAC

- Chaque machine est identifiée par une clé globalement **unique**, appelée **adresse MAC**, pour s'assurer que toutes les machines (plus précisément interfaces Ethernet) sur un réseau Ethernet ont des adresses distinctes

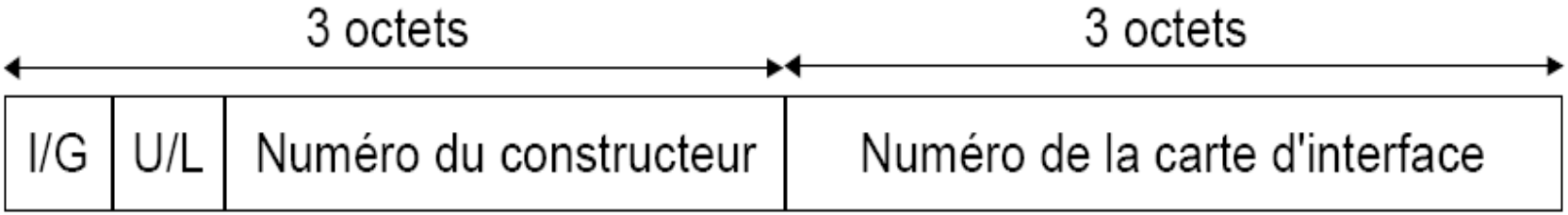
- Une adresse MAC est une adresse matérielle, c'est-à-dire une adresse unique stockée sur une mémoire morte (ROM) de la carte réseau.

- Adressage standardisé par l'IEEE 802

Les adresses MAC

- Les adresses MAC comportent 48 bits (6 octets) et sont exprimées sous la forme de 12 chiffres hexadécimaux :
  - 6 chiffres sont administrés par l'IEEE et identifient le fabricant de la carte
  - 6 chiffres forment le numéro de série de la carte

- **Exemple :** 00-00-0c-12-34-56



Format des adresses MAC : adresses uniques et de groupes

Interprétation du début des adresses MAC : exemples
(source : http://standards.ieee.org)

Code fabricant (OUI) sur 3 octets, en hexadécimal	Vendeur / fabricant
00 - 00 - 0C	Cisco
00 – 03 – 93	Apple
02 – 80 - 8C	3Com
08 – 00 – 20	Sun
08 – 00 - 5A	IBM

Adresses de groupe (bit I/G à 1)

Adresse(s) MAC	Type	Description
FF-FF-FF-FF-FF-FF	*Broadcast*	Diffusion généralisée
01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF	*Internet multicast* (RFC 1112)	Diffusion restreinte

Liste des constructeurs de carte réseau : http://www.frameip.com/ethernet-oui-ieee/

Accès au medium de transmission

- Les **collisions de transmissions** sont le principal problème à régler.
- Elles se produisent lorsque deux (ou plus) stations essaient de transmettre en même temps.
- Les messages se superposent et il devient impossible d'en reconnaître le contenu exact.
- Une station peut penser que le médium est libre alors qu'une transmission est déjà commencée.
- Lorsque les messages se superposent, les stations émettrices s'en aperçoivent et mettent fin à leur émission.
- Plus le nombre de stations reliées au réseau est grand et plus celui-ci est étendu (délais plus longs), plus la probabilité de collision sera grande.

Méthodes d'accès

- Accès aléatoire
  - CSMA/CD (Collision detection) : Ethernet
  - CSMA/CA (Collision avoidance) : Wifi

- Accès déterministe : une machine a le droit d'émettre si elle possède le jeton.
  - Token ring : le jeton circule dans l'ordre physique des stations.
  - Token bus : le jeton circule dans l'ordre logique des stations.

Aloha

Dans les années 70, l'université d'Hawaï établit une réseau radio terrestre entre 8 îles.

- **Aloha pur :**
  - Toute station qui veut émettre, accède librement au canal.
  - Lorsqu'il y a collision, arrêt d'émission pendant un temps aléatoire puis réémission.

- **Aloha discrétisé :**
  - Division du temps en slots constants
  - Émission seulement au début d'un slot
  - Pas de collision ou collision complète du message

Ethernet : Méthode d'accès CSMA/CD

- **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection
  - **CSMA** : avant d'émettre, l'émetteur « écoute » le support de transmission (= canal), afin de détecter des émissions en cours
  - **CD** : l'émetteur s'aperçoit qu'un autre nœud est en train d'envoyer un message au même moment que lui (= collision)

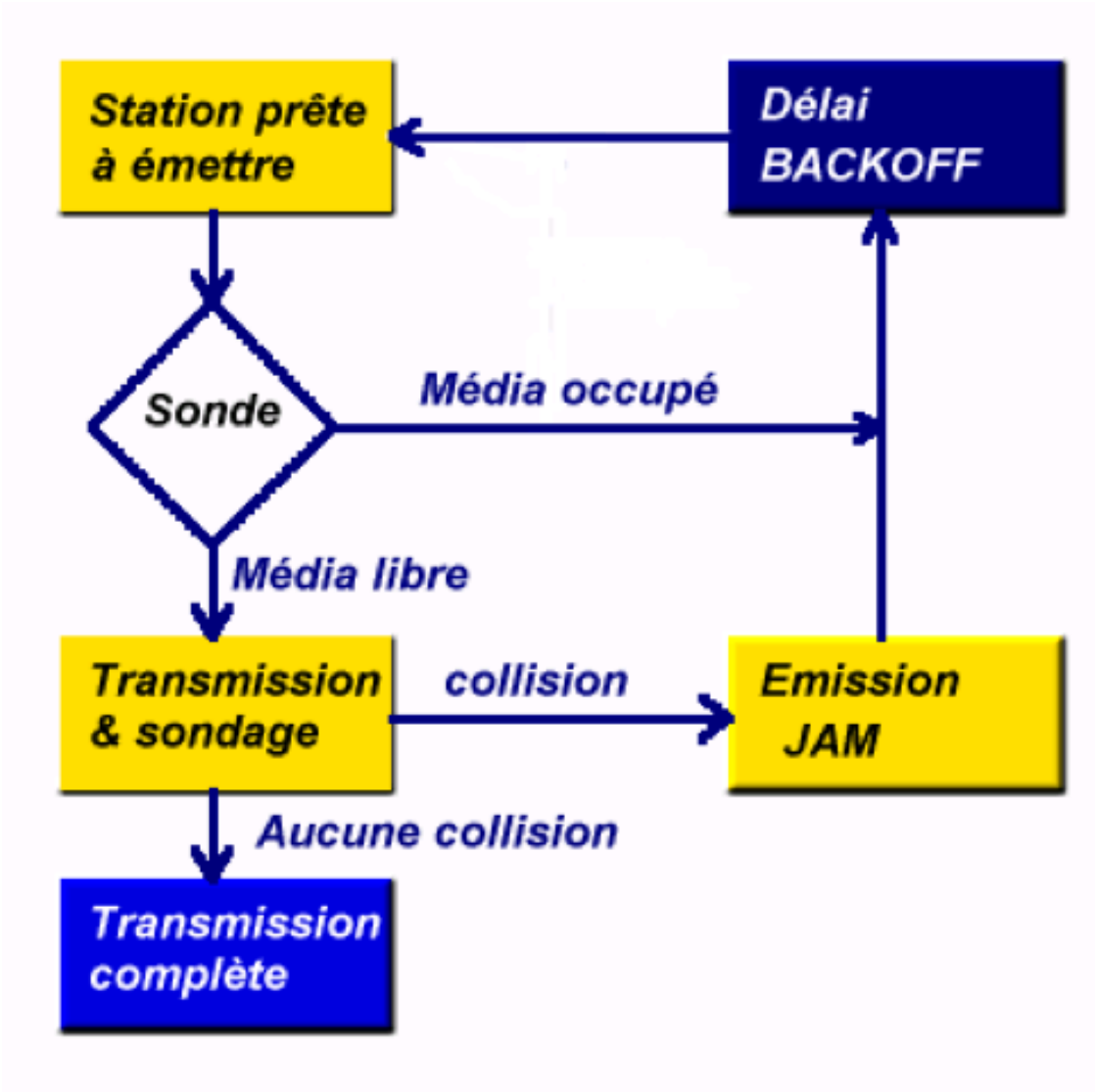
- Collision = brouillage des trames et réception incorrecte
  → les trames doivent être émises à nouveau

- Collision Detection : méthode non adaptée aux réseaux sans fil (ex. 802.11), pas d'écoute possible pendant l'émission

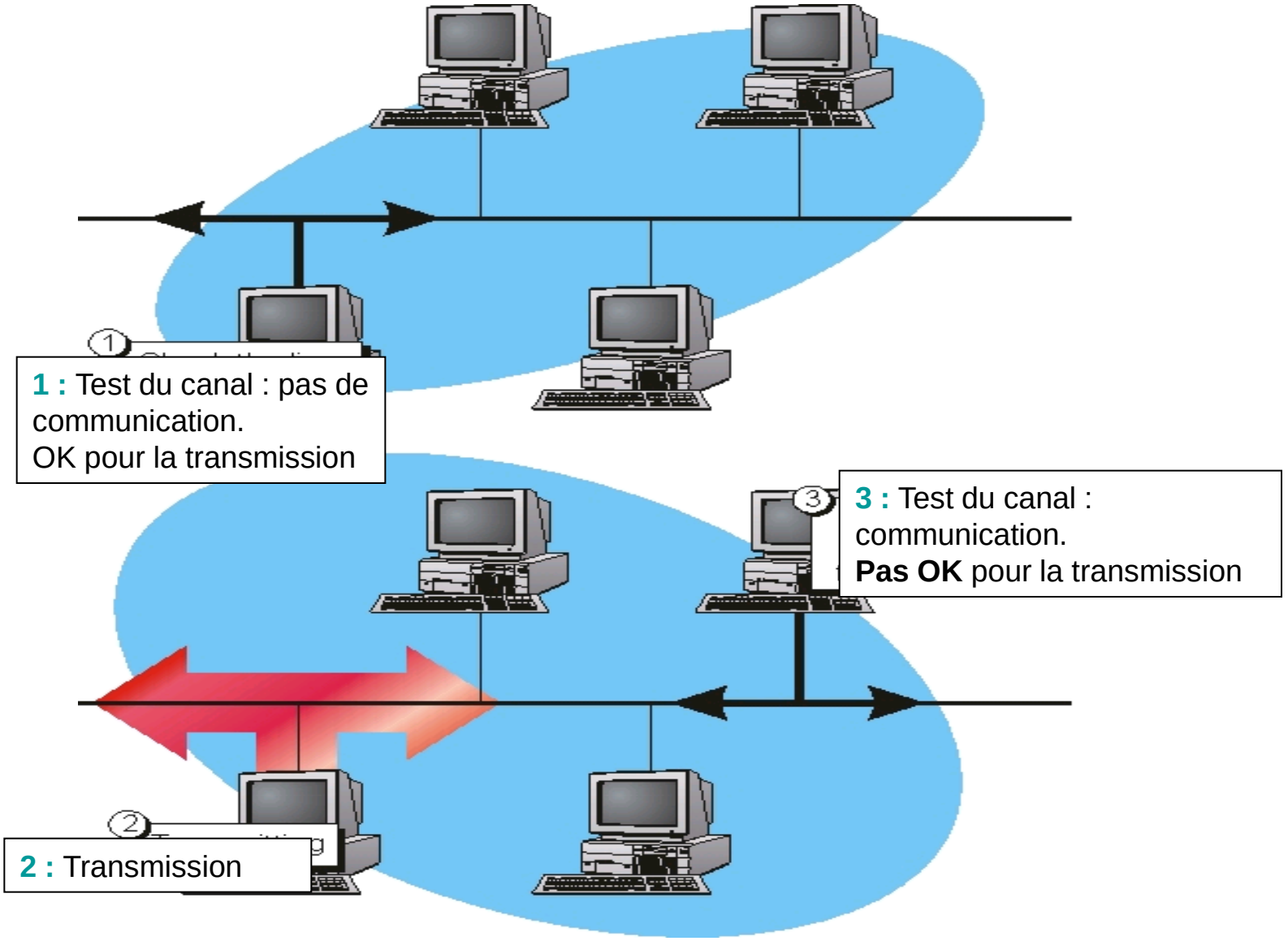
Méthode CSMA/CD : principe du fonctionnement

- Si le canal est libre, alors émettre une trame
- Si le canal est occupé, attendre sa libération et émettre aussitôt il se libère
- Si l'on détecte une collision durant l'émission :
  1. Arrêter l'émission
  2. Attendre un temps aléatoire avant de réessayer (retour à 1)
- Si le nombre de collisions dépasse un certain seuil, on considère qu'il y a une erreur fatale et l'émission s'interrompt avec la condition excessive collisions

CSMA/CD


Station prête à émettre
Délai BACKOFF
Sonde
Média occupé
Média libre
Transmission & sondage
collision
Emission JAM
Aucune collision
Transmission complète

CSMA/CD


1 : Test du canal : pas de communication.
OK pour la transmission
3 : Test du canal : communication.
Pas OK pour la transmission
2 : Transmission

Evolutions Ethernet Commuté

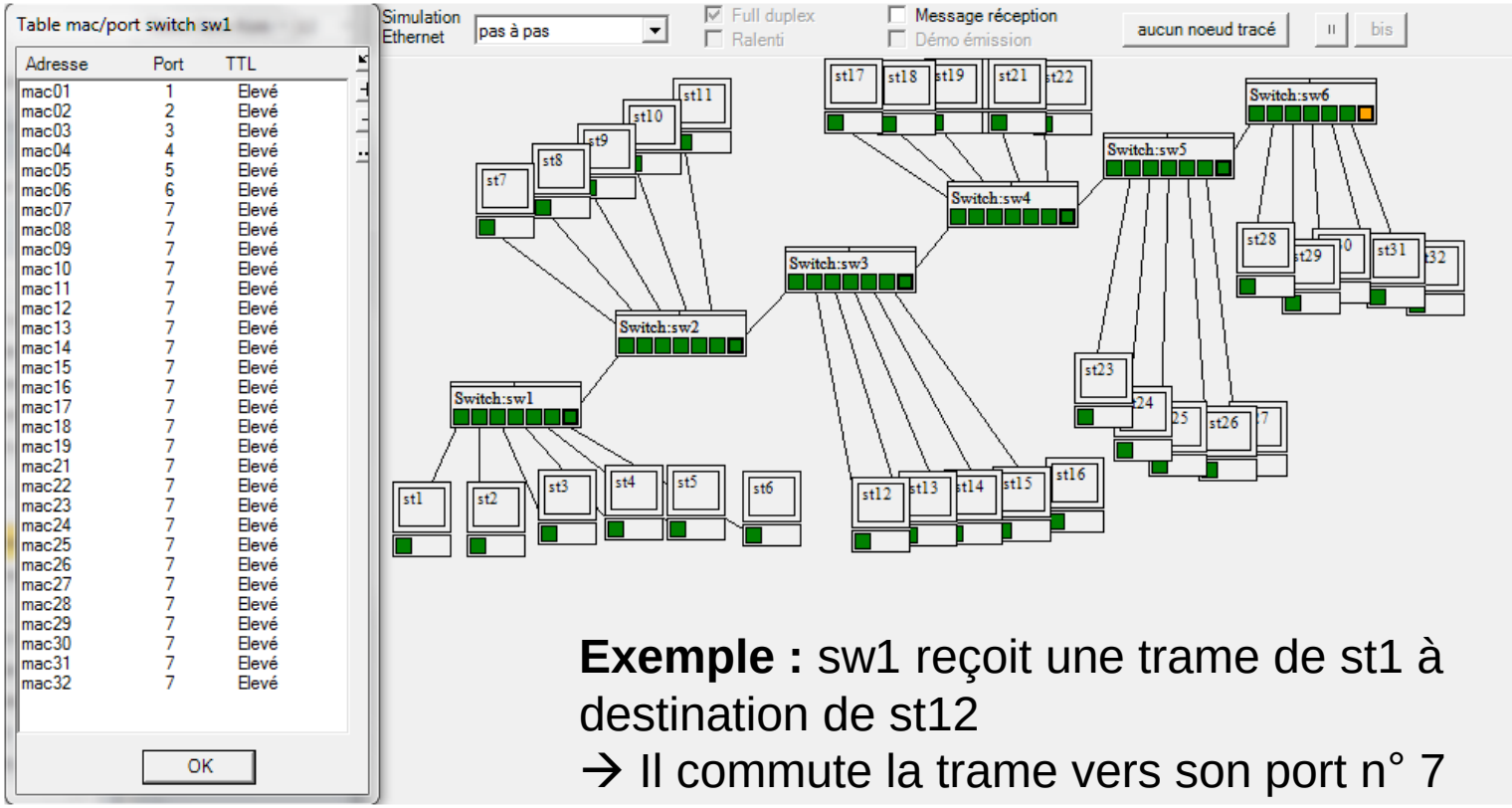
- **Vitesses** : de 10 Mbit/s à 100 Mbit/s, 1 Gbit/s..
- Grâce à l'utilisation de commutateurs :
  - **Commutation** : disparition des collisions, augmentation du débit, sécurité accrue
  - **VLAN** (Virtual LAN) : permettent de regrouper les nœuds dans des groupes séparés pour des aspects de sécurité et de gestion administratives

Switch (Commutateur)

- Equipement au niveau liaison
- Permet d'offrir plus de la bande passante par rapport au cas où les nœuds partagent le même canal de communication
- Reçoit les trames d'un port et l'envoie juste vers la porte (entrée/sortie) connectant avec la destination correspondante en se basant sur l'adresse MAC
- Utilise la table de contenant les adresses MAC et les sorties correspondantes

Commutation

- Le switch choisit pour chaque trame reçue un port de sortie menant a sa destination finale en fonction de la table mac/port



Exemple : sw1 reçoit une trame de st1 à destination de st12
→ Il commute la trame vers son port n° 7

Le commutateur (1)

- Inspecte les adresses de source et de destination des messages,
- Table qui permet alors de savoir quelle machine est connectée sur quel port du switch (remplie automatiquement, mais réglages complémentaires manuels possibles).
- Connaissant le port du destinataire, le commutateur ne transmettra le message que sur le port adéquat, les autres ports restants dès lors libres pour d'autres transmissions pouvant se produire simultanément.
- Chaque échange peut s'effectuer
  - à débit nominal (plus de partage de la bande passante),
  - sans collisions, avec pour conséquence une augmentation très sensible de la bande passante du réseau (à vitesse nominale égale).

Le commutateur (2)

- Puisque la commutation permet d'éviter les collisions et que les techniques 10/100/1000 base T(X) disposent de circuits séparés pour la transmission et la réception (une paire torsadée par sens de transmission), la plupart des commutateurs modernes permet de désactiver la détection de collision et de passer en mode full-duplex sur les ports
  → les machines peuvent émettre et recevoir en même temps

- Le mode full-duplex est particulièrement intéressant pour les serveurs qui doivent desservir plusieurs clients.

- Comme le trafic émis et reçu n'est plus transmis sur tous les ports, il devient beaucoup plus difficile d'espionner (sniffer) ce qui se passe → Sécurité accrue

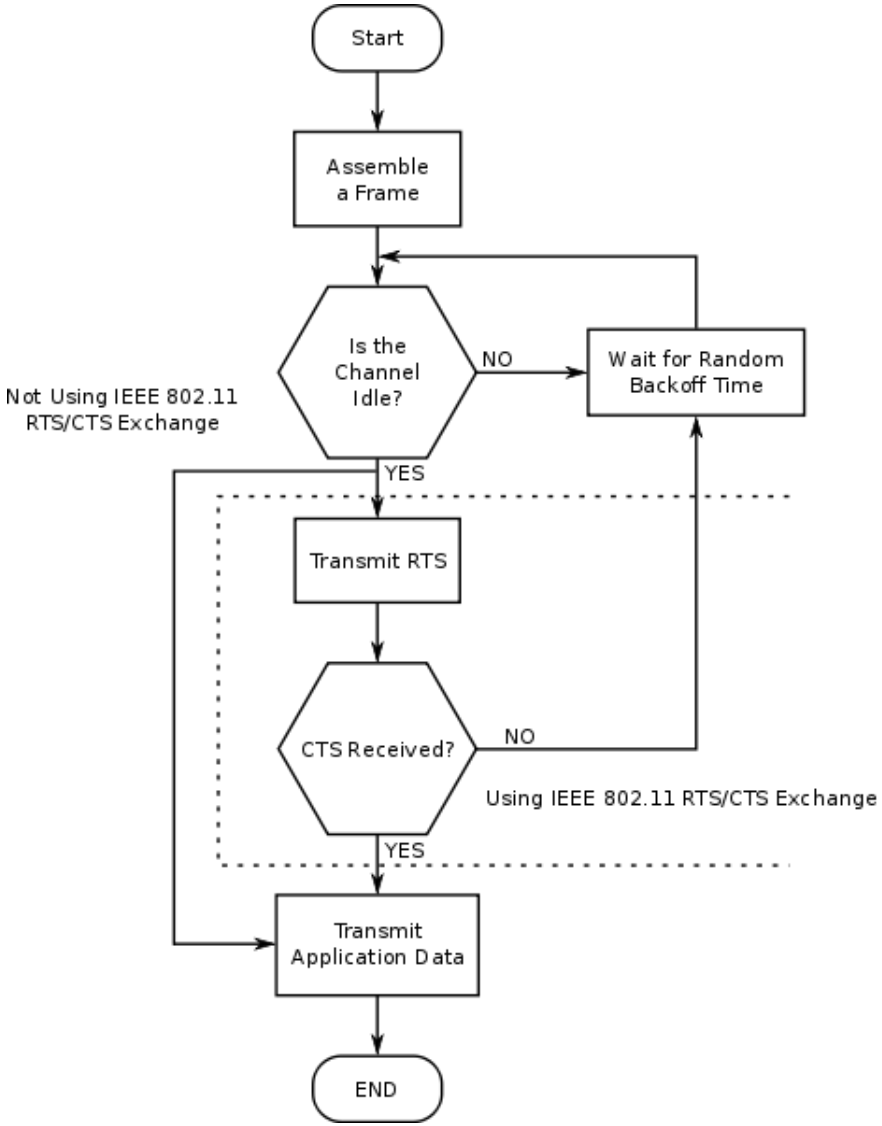
CSMA/CA (dans les réseaux sans-fils)

- Dans un environnement sans fil CSMA/CD ne peut pas être appliqué car on ne peut pas détecter les collisions en même temps que l'on émet.
- Ainsi la norme 802.11 propose **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*).
- Le protocole *CSMA/CA* utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur.

CSMA/CA (2)

- La station voulant émettre écoute le réseau.
- Si le réseau est encombré, la transmission est différée.
- Si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut émettre :
  1. La station transmet un message appelé *Ready To Send* (*RTS*) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.
  2. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*), puis la station commence l'émission des données.
  3. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (*ACK*).
  4. Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

CSMA/CA (3)



http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withouthidden.html

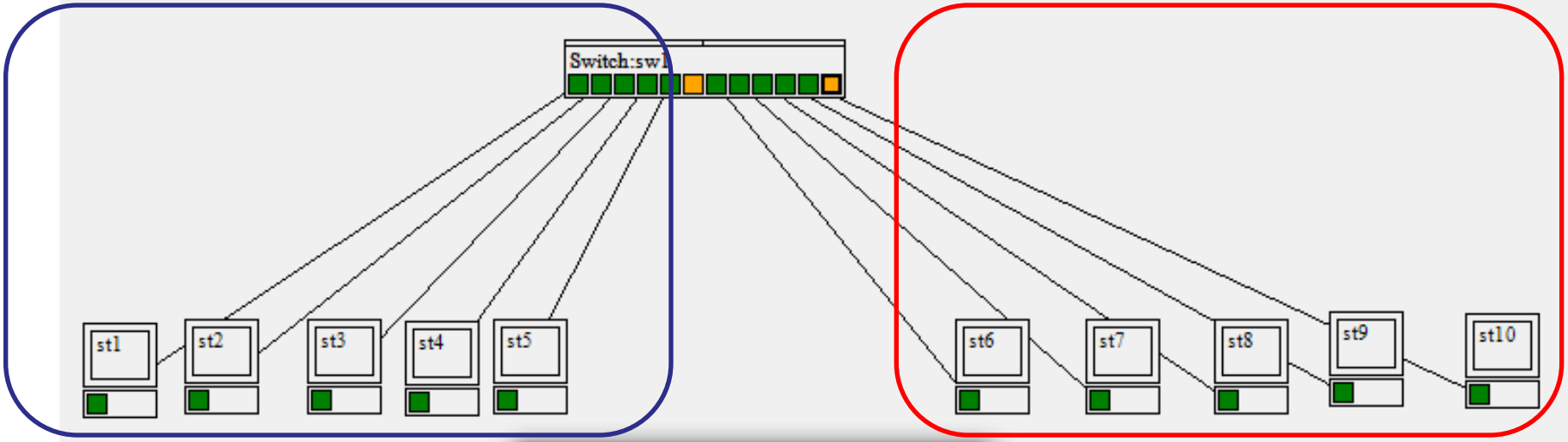
VLAN (*Virtual Local Area Network*)

- Un VLAN est un ensemble d'unités regroupées quelque soit l'emplacement de leur segment physique
- Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :
  - Plus de souplesse pour l'administration et les modifications du réseau (e.g. mobilité) car toute l'architecture peut être modifiée par simple paramètrage des commutateurs
  - Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
  - Réduction de la diffusion du trafic sur le réseau

Types de VLAN

- VLAN statique : les ports du commutateur sont affectés aux différents VLAN
  - Facilité d'administration
  - Fonctionnent bien dans les réseaux où les déplacements sont contrôlés et gérés
- VLAN dynamique : les ports des commutateurs peuvent automatiquement déterminer leur VLAN d'appartenance. Filtrage basé sur :
  - Les adresses MAC
  - L'adressage IP
  - D'autres paramètres
- Cette méthode est celle qui demande le moins d'administration au niveau du local technique
- VLAN de niveau 1 et de niveau 2

VLAN



VLAN 1

VLAN 2

Table port/vlan switch sw1

Port	Vlan
01	1
02	1
03	1
04	1
05	1
06	1
07	2
08	2
09	2
10	2
11	2
12	1

CRC (Cyclic Redundancy Code) : contrôle d'erreurs (1)

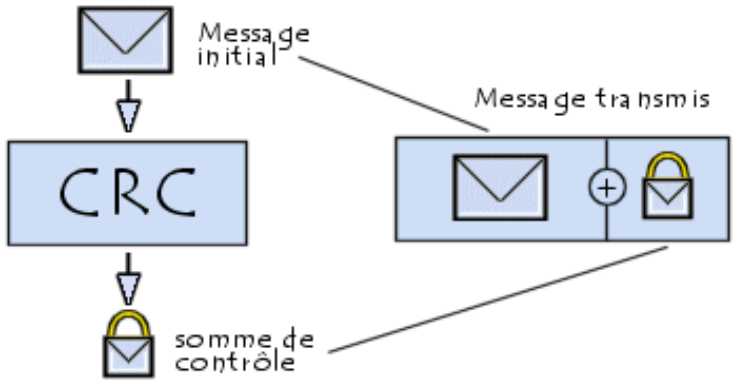
Le **contrôle de redondance cyclique** consiste à protéger des blocs de données afin de s'assurer que l'information reçue est conforme à l'information envoyée.

- A chaque trame est associé un bloc de données, qui contient des éléments redondants vis-à-vis de la trame, permettant de détecter les erreurs, mais aussi de les réparer.

CRC (Cyclic Redundancy Code) : contrôle d'erreurs (2)

- Le CRC représente une fonction mathématique (un binôme) redonnant une valeur calculée sur la valeur binaire du paquet, cette valeur étant calculée par l'équipement expéditeur pour chaque paquet envoyé et ajouté à la fin des paquets.

- L'équipement récepteur calcule à son tour le CRC: si la valeur correspond au CRC reçu, il considère le paquet comme dépourvu d'erreur; dans le cas contraire, il ne le réceptionne pas.



CRC (Cyclic Redundancy Code) : contrôle d'erreurs (3)

- Il peut demander immédiatement le renvoi du paquet en erreur, ce qui provoque un trafic important (accusé de réception (*aknowledgment*)).

- Il peut attendre l'arrivée d'un certain nombre de paquets, et demander ensuite le renvois des paquets en erreur (TCP/IP). Cette méthode génère un trafic moins important, puisqu'un seul paquet d'accusé de réception est envoyé pour un certain nombre de paquets reçus (ce nombre varie en fonction de la taille de la *fenêtre de réception*).

- Il peut ignorer l'événement, valider le paquet, et laisser les applications gérer le problème (en provoquant une erreur, dans le pire des cas...): par ex. UDP/IP.

Types de câbles éthernet les plus courants

Nom	Type	Longueur maximale d'un segment	Nombre de nœuds par segment	Remarques
10Base5	Coaxial épais	500 m	100	Câble original, maintenant obsolète
10Base2	Coaxial fin	185 m	30	Pas de hub nécessaire
10Base-T	Paire torsadée	100 m	1024	Système le moins cher
10Base-F	Fibre optique	2000 m	1024	Le mieux adapté pour relier les immeubles

V - Couche Réseau : IP, ICMP, ARP

Couche réseau

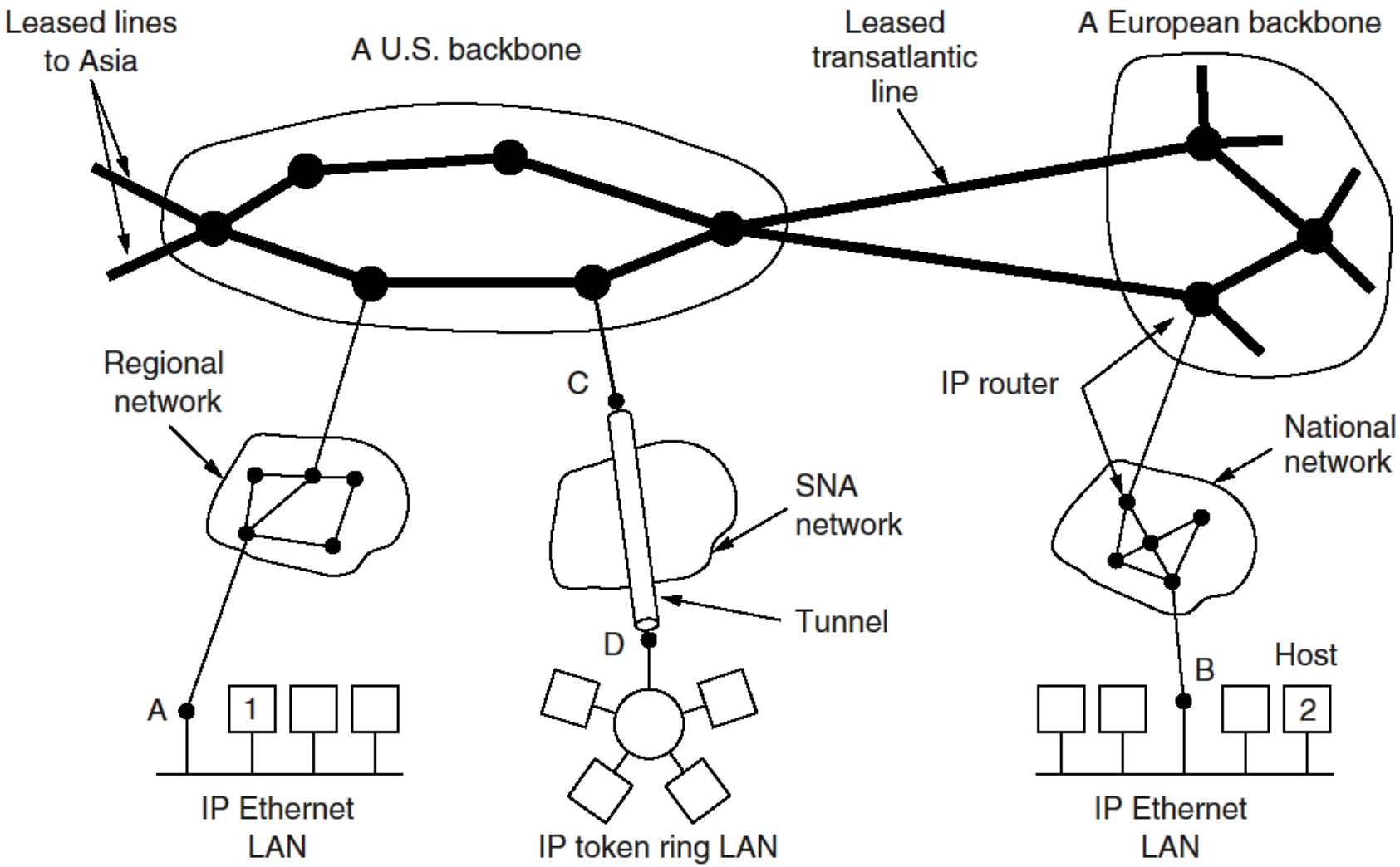
- Assure l'acheminement des données de la source à la destination à travers un ou plusieurs des réseaux de communication intermédiaires entre les 2 systèmes terminaux.
- Unité d'information : le paquet
- Localisation des systèmes : adressage logique des nœuds et routage (trouve une route entre la source et la destination)
- Contrôle le flux des données acheminées : optimisation du réseau
- Détecte et corrige les erreurs non réglées par la couche 2

- **Exemples :**
  - X25 (couvrant les 3 couches inférieures), IP (Internet Protocol).

La couche Réseau

- Acheminer les données entre l'émetteur et le destinataire à travers de différents réseaux en mettant en place un système **d'adressage hiérarchique.**
- C'est la première couche de **bout en bout**
- Les problèmes à traiter :
  - **Routage** : pour toutes paires d'adresses : trouver un chemin entre les 2 machines. Extension à un groupe d'adresses (diffusion, multicast). Routage.
  - **Annuaires** : Nommer (désigner) les machines : adresses réseaux, noms.

Internet : interconnexion de réseaux

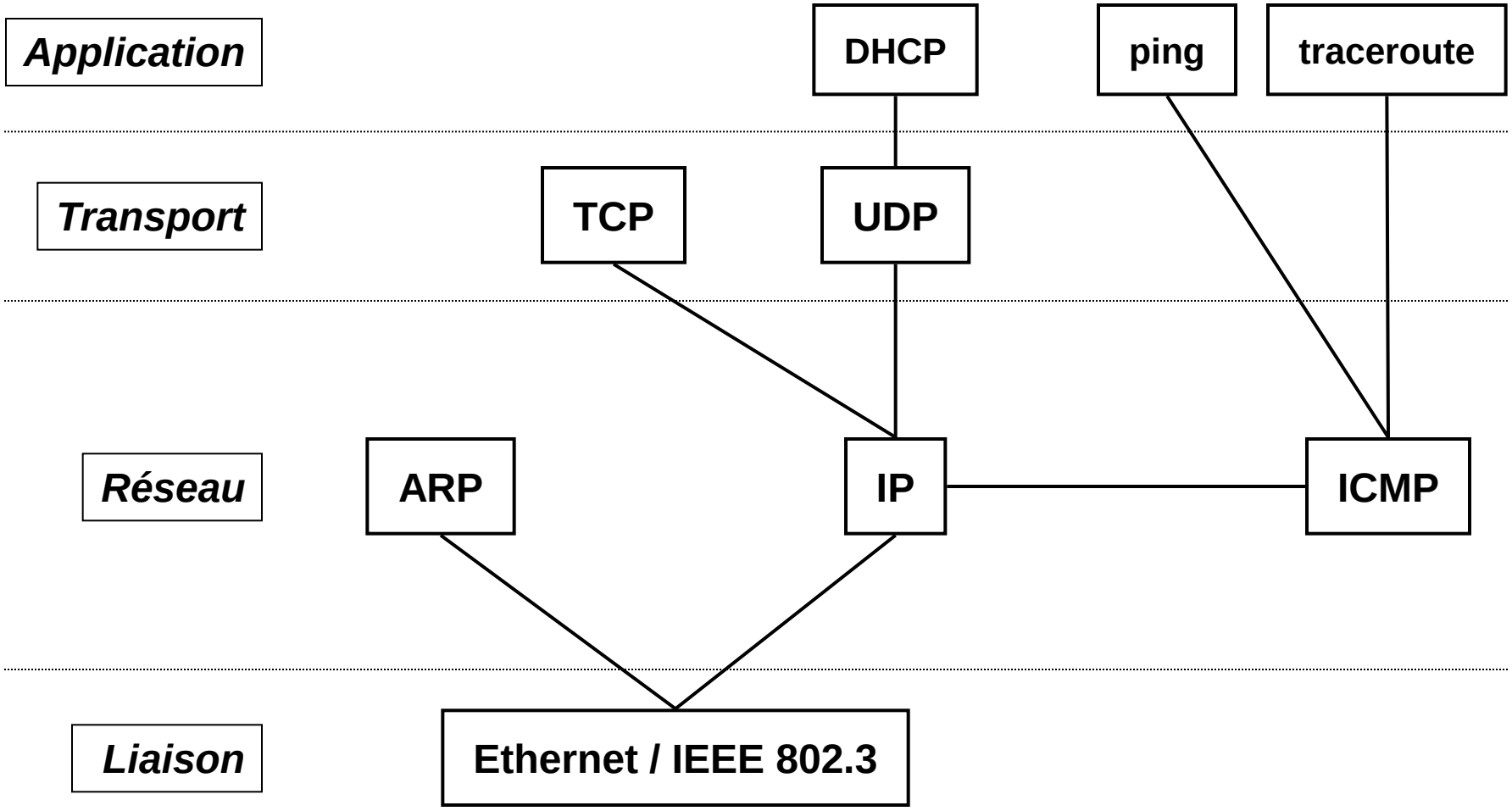


Internet et IP

- **Internet** = ensemble de réseaux (Autonomous Systems) connectés entre eux

- **IP** = Internet Protocol. Deux versions incompatibles entre elles :
  - **IPv4** : version la plus courante aujourd'hui
  - **IPv6** : IP « nouvelle génération »

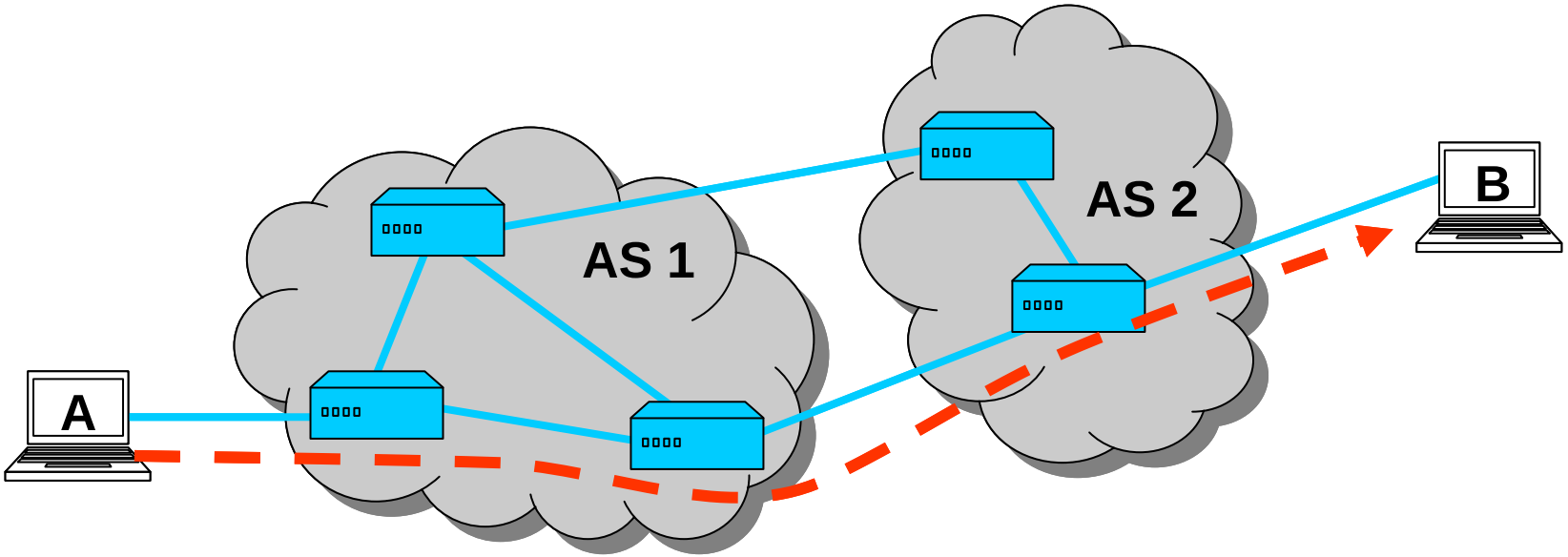
Couche 3 : architecture simplifiée



Qu'offre IP aux couches supérieures ?

- Un service à « datagrammes »
  - Acheminement des paquets de la source à la (aux) destination(s)
  - Service non orienté connexion
    - Deux paquets consécutifs peuvent suivre une route différente pour aller de A à B
  - Service non fiable : « best effort »
    - Perte de paquets : possible
    - Duplication de paquets : possible
    - Arrivée des paquets en séquence : non garantie

Interconnexion de réseaux IP

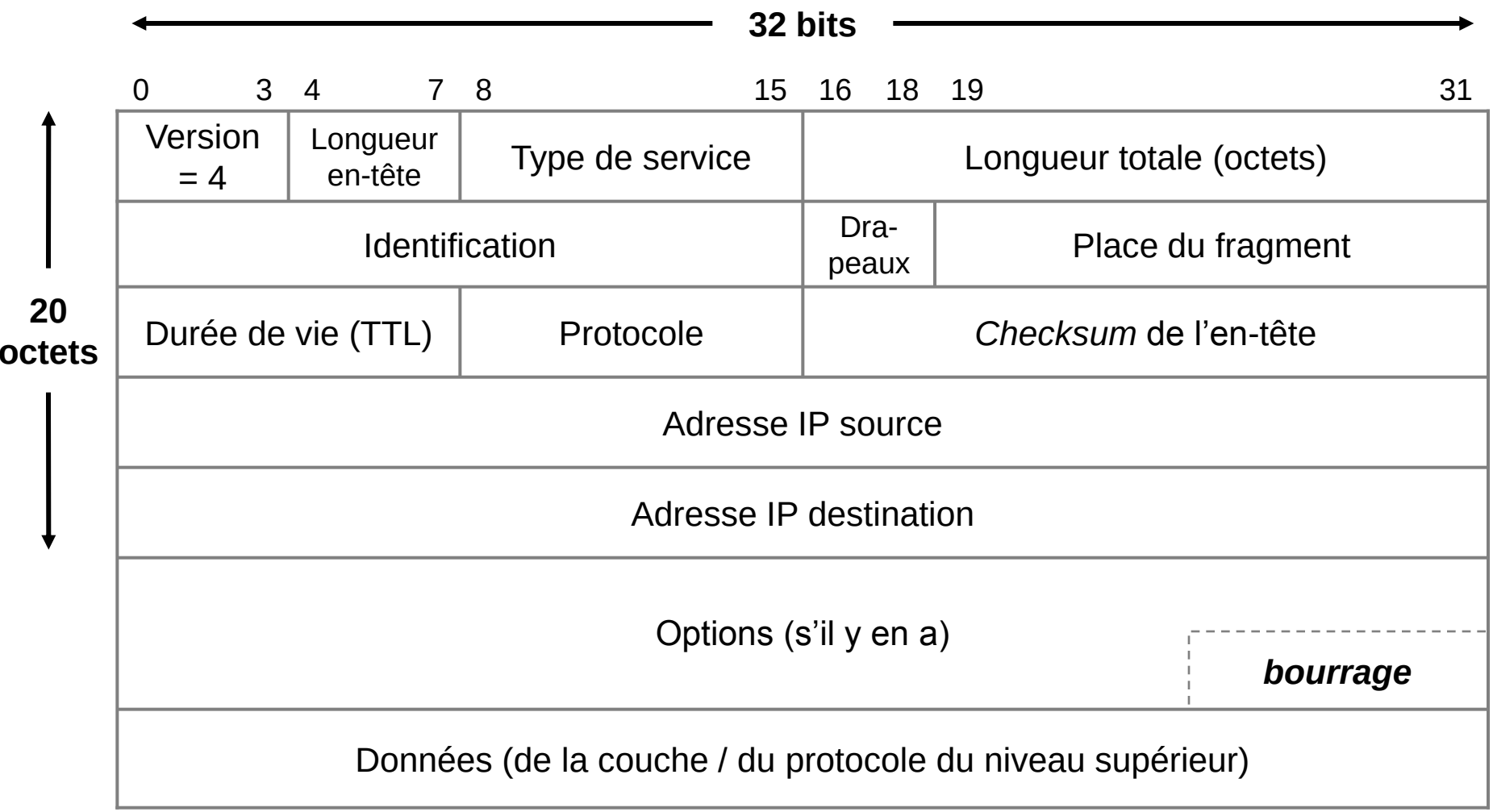


- Adresses avec signification globale
- Relayage des paquets IP
  - Analyse des adresses (contenues dans l'en-tête IP)
  - Table de routage : quel est le prochain routeur sur le chemin ?

Comparaison commutation de datagrammes et commutation de circuit virtuel

Aspect	Datagrammes	Circuit virtuel
Phase d'établissement	Pas nécessaire	Requise
Adressage	Chaque paquet contient les adresses source et destination	Chaque connexion requiert des informations d'identification de circuit dans la table de routage
Routage	Chaque paquet est routé indépendamment	La route est choisie lors de l'établissement du circuit et tous les paquets suivent la même route
Impact d'une panne de routeur	Aucun, à part pour les paquets perdus au moment de l'incident	Tous les CV passant par ce routeur sont supprimés
Qualité de service et contrôle de congestion	Difficile à garantir	Facile à garantir si on peut allouer suffisamment de ressources à chaque CV

Format d'un paquet IPv4



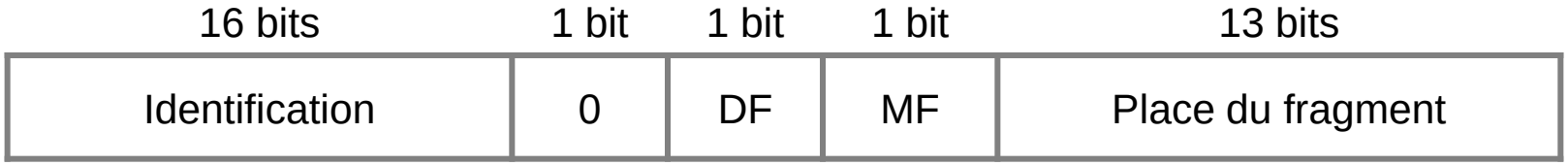
Fragmentation

- La fragmentation d'un datagramme se fait au niveau des routeurs
- Si la MTU (*Maximum Transmission Unit*) de la liaison ne permet de transporter le paquet entier : envoi du paquet en fragments
- Le réassemblage est fait uniquement par le destinataire final
- Mécanisme coûteux pour les routeurs
- N'existe plus en IPv6

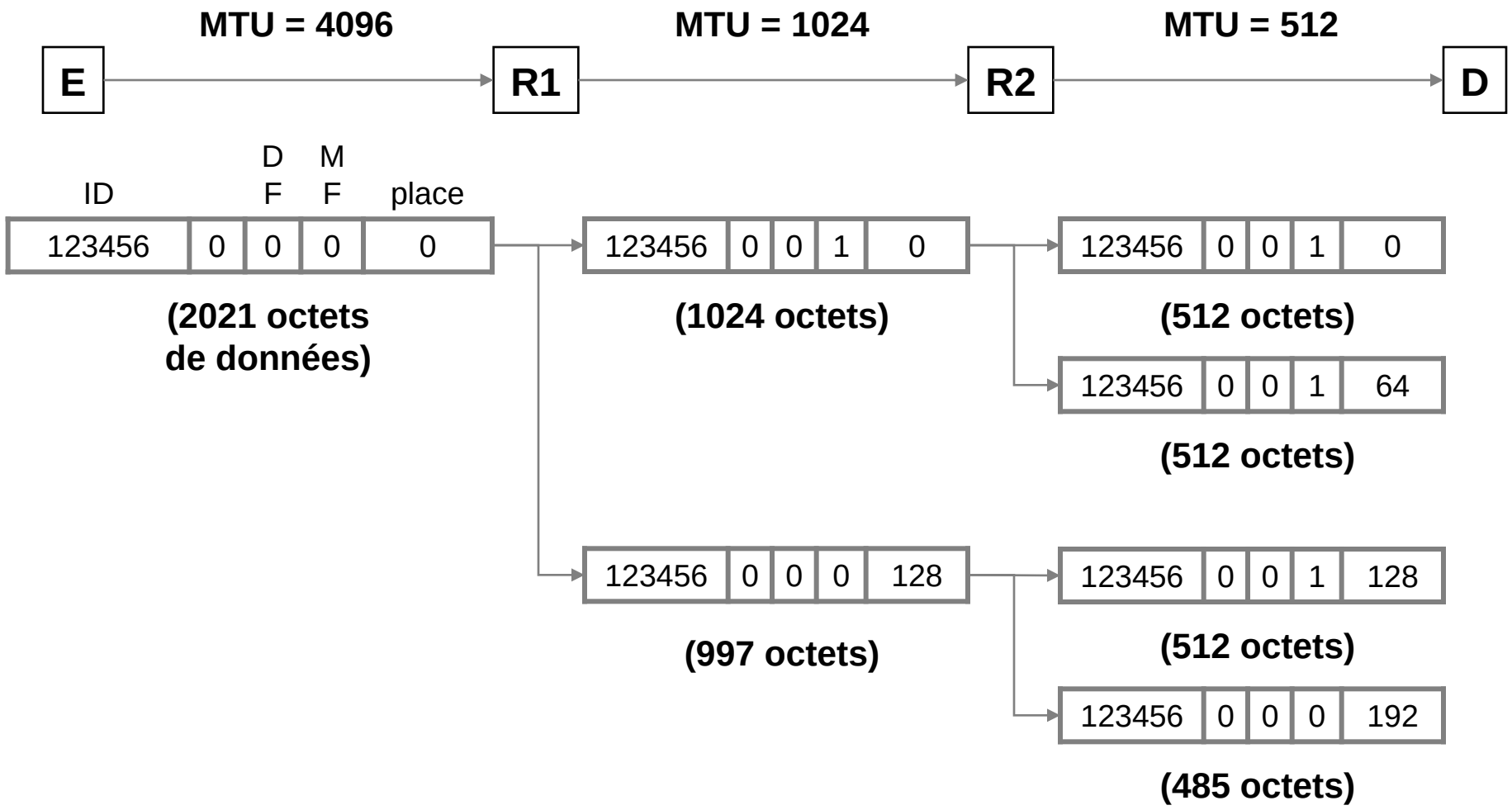
Dessin : [Tanenbaum, 2002]

Fragmentation : champs de l'en-tête

- **Identification** : numéro unique (pour l'émetteur)
  - Si le paquet est fragmenté après, tous les fragments le portent
- **Place du fragment** : position du 1er octet du fragment dans le datagramme original (non fragmenté)
  - Découpe des fragments en multiples de 8 octets
- **DF** (*don't fragment*) = 1 ⇨ le paquet ne doit pas être fragmenté
  - Si fragmentation nécessaire : écartement du paquet + génération d'un message ICMP vers la source
- **MF** *(more fragments)*
  - MF = 0 dernier fragment
- Drapeaux par défaut (paquet non fragmenté) : DF = MF = 0



Fragmentation : exemple



Champ **Durée de vie (TTL)**

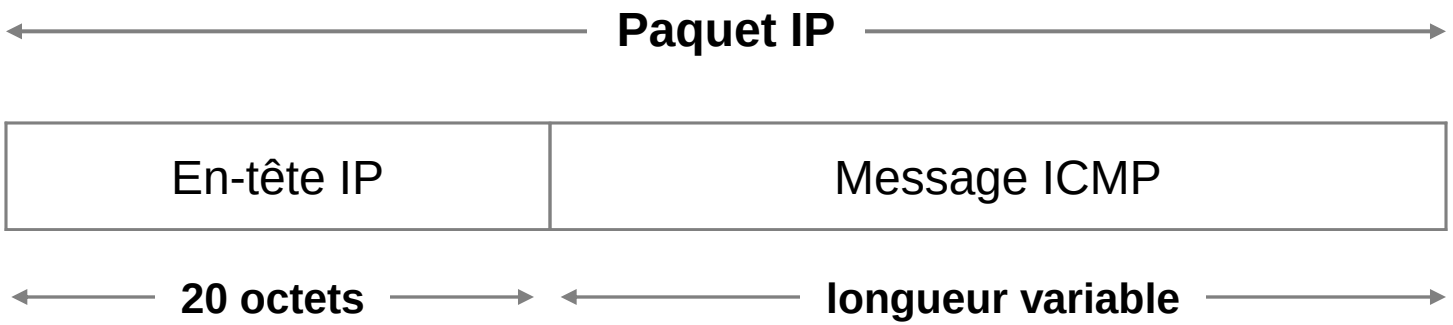
- Initialisé à une valeur > 0
  - Valeur typique = 64
- Décrémenté d'une unité :
  - À chaque fois que le paquet traverse un routeur
  - Une fois/sec, si le paquet est en attente de réassemblage dans la station destinataire
- Quand TTL = 0, le paquet est détruit par le routeur et une notification (ICMP) est envoyé à l'émetteur du paquet

- **But :** éviter que les paquets bouclent indéfiniment dans le réseau si il y a des erreurs dans les tables de routage par exemple.

Couche réseau : protocole ICMP

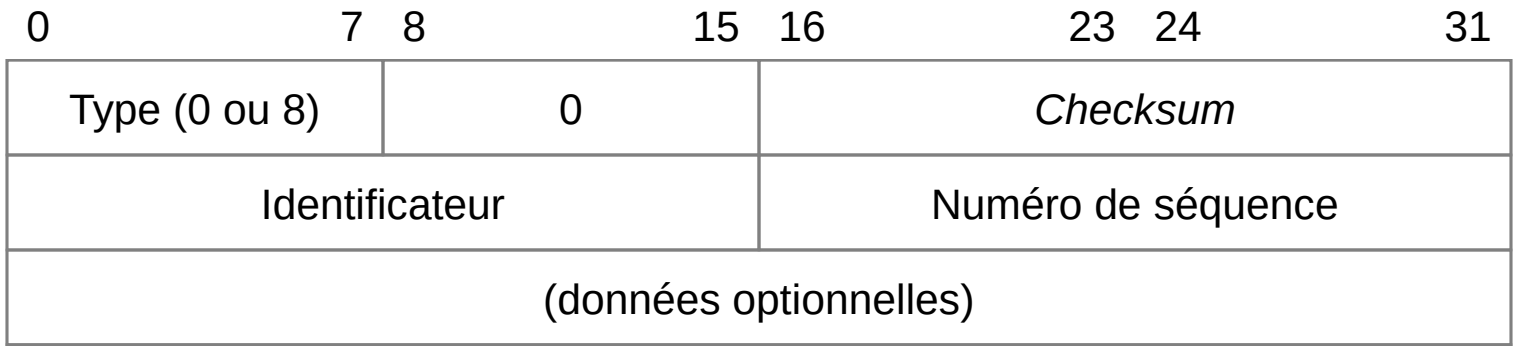
Protocole ICMP

- *Internet Control Message Protocol* (RFC 792)
- But : échange de messages d'erreur et de demande d'information
  - Traités soit par IP, soit par une couche supérieure
- Niveau 3, mais encapsulé dans des paquets IP
  - Champ *Protocole* = 1



Commande *ping*

- Basée sur les messages ICMP de type 8 (*echo request*) et 0 (*echo reply*)
  - Réception d'un message type 8 ⇒ émission d'un message type 0
- Format des messages



La réponse contient une copie des champs *Identificateur*, *N° de séquence* et les données optionnelles

Quelques types de messages ICMP

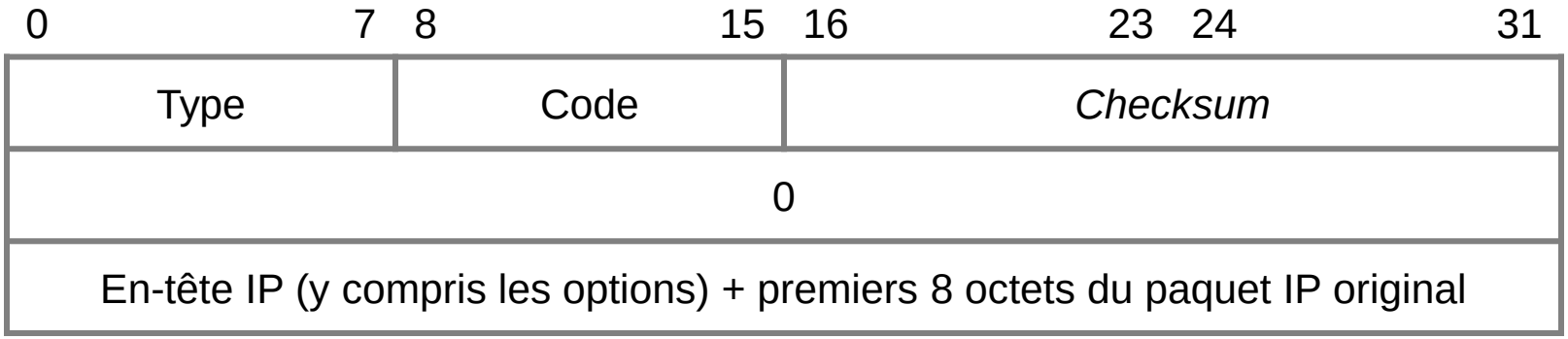
Type	*Code*	*Description*	*Demande*	*Erreur*
0	0	Réponse à une demande d'écho	🗐	
3		Destination non accessible :		
	0	Réseau inaccessible		🗐
	1	Station inaccessible		🗐
	2	Protocole inaccessible		🗐
	3	Fragmentation nécessaire mais bit DF = 1		🗐
	4	Port inaccessible		🗐
		etc.		
8	0	Demande d'écho	🗐	
11		La durée de vie (TTL) a atteint 0 :		
	0	Durant le transit		🗐
	1	Durant le réassemblage		🗐

ping

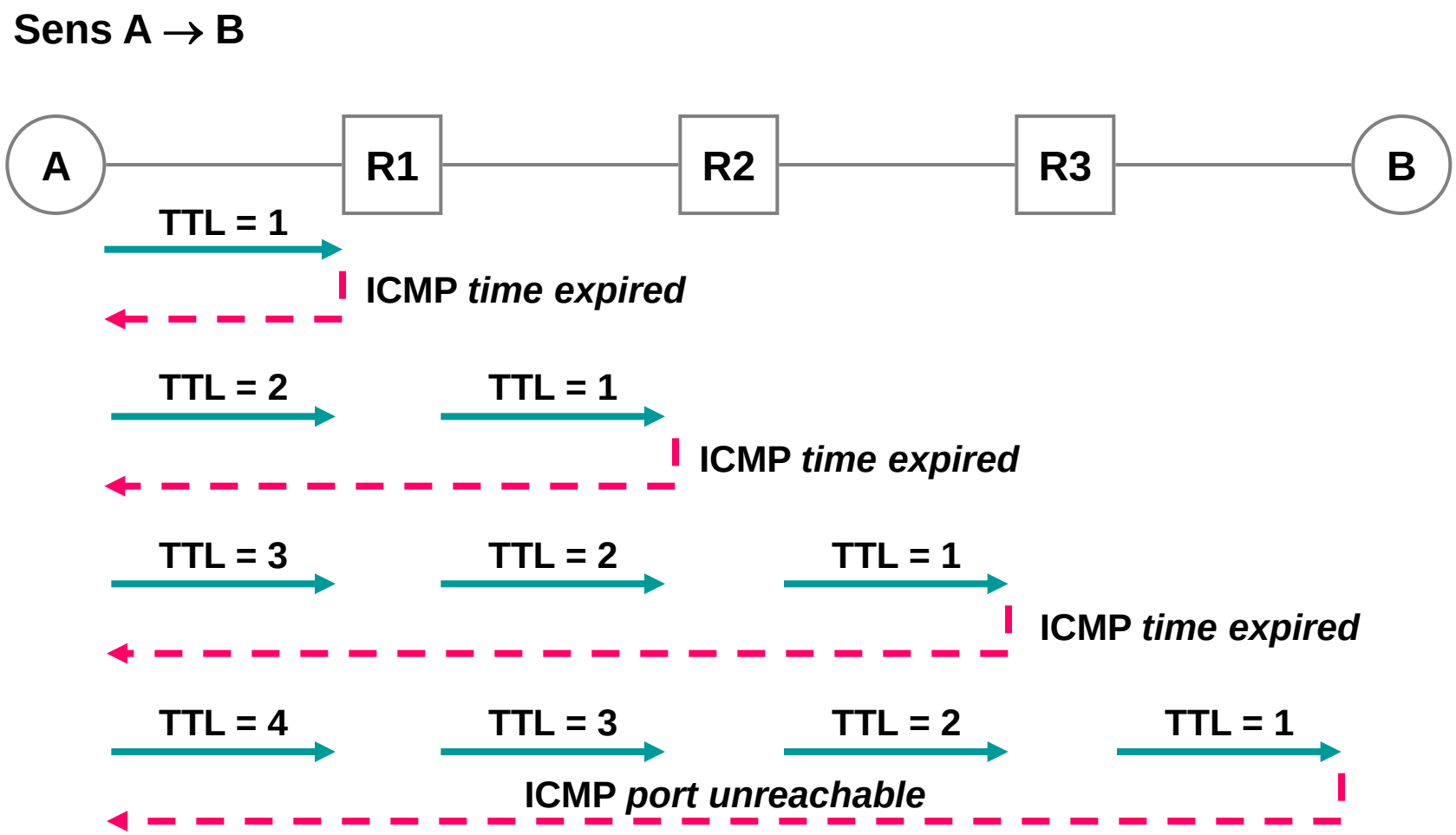
```
Z:\>ping www.google.fr

Envoi d'une requête 'ping' sur www.l.google.com [209.85.135.103] avec 32 octets
de données :

Réponse de 209.85.135.103 : octets=32 temps=31 ms TTL=241
Réponse de 209.85.135.103 : octets=32 temps=32 ms TTL=241
Réponse de 209.85.135.103 : octets=32 temps=32 ms TTL=241
Réponse de 209.85.135.103 : octets=32 temps=32 ms TTL=241

Statistiques Ping pour 209.85.135.103:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 31ms, Maximum = 32ms, Moyenne = 31ms

Z:\>
```

tracert

- Basé sur les messages ICMP de type 11 / code 0 (*time exceeded*) et type 3 / code 4 (*port unreachable*)



tracert : fonctionnement

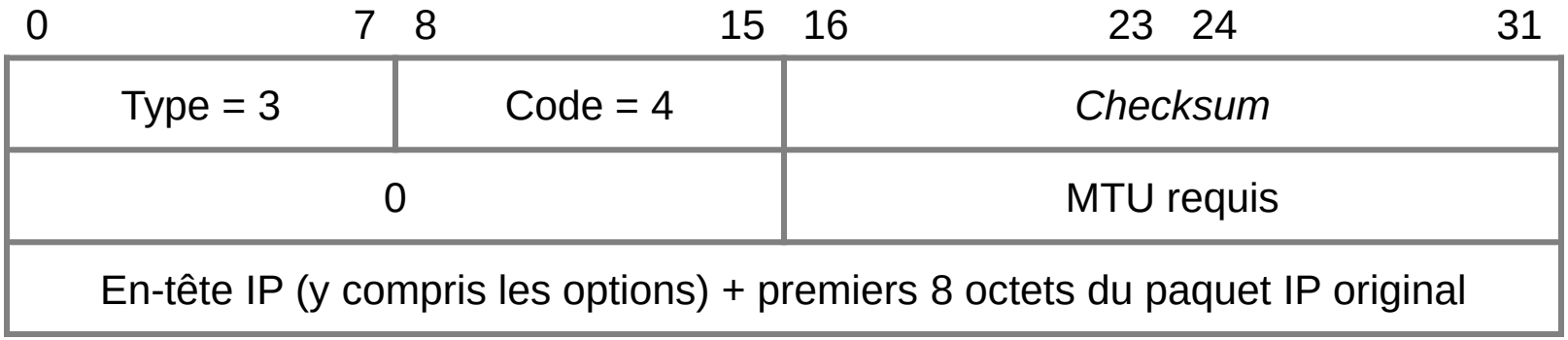


tracert

```
Z:\>tracert www.google.fr

Détermination de l'itinéraire vers www.l.google.com [209.85.135.103]
avec un maximum de 30 sauts :

  1     1 ms    <1 ms    <1 ms  sophia-p32.inria.fr [138.96.32.250]
  2    <1 ms    <1 ms    <1 ms  nice-g3-0-60.cssi.renater.fr [193.51.181.138]
  3    15 ms    15 ms    15 ms  marseille-pos4-0.cssi.renater.fr [193.51.179.245
]
  4    15 ms    15 ms    15 ms  montpellier-pos2-0.cssi.renater.fr [193.51.179.2
42]
  5    15 ms    15 ms    15 ms  lyon-pos14-0.cssi.renater.fr [193.51.179.221]
  6    14 ms    14 ms    14 ms  nri-b-pos9-0.cssi.renater.fr [193.51.179.13]
  7    15 ms    15 ms    15 ms  TELEGLOBE-FRANCE-INTERNATIONAL.sfinx.tm.fr [194.
68.129.242]
  8    15 ms    15 ms    15 ms  if-6-0-7.core1.PV1-Paris.teleglobe.net [80.231.7
9.14]
  9    24 ms    24 ms    24 ms  if-2-0-0.core2.FR1-Frankfurt.teleglobe.net [80.2
31.65.65]
 10    32 ms    35 ms    35 ms  12.icore1.FR1-Frankfurt.teleglobe.net [80.231.65
.6]
 11    24 ms    25 ms    25 ms  195.219.180.30
 12    25 ms    49 ms    25 ms  209.85.249.178
 13    31 ms    31 ms    31 ms  209.85.248.248
 14    31 ms    36 ms    31 ms  72.14.239.46
 15    38 ms    35 ms    33 ms  72.14.239.58
 16    32 ms    31 ms    32 ms  mu-in-f103.google.com [209.85.135.103]

Itinéraire déterminé.

Z:\>_
```

Path MTU

- Découverte de la taille maximale des paquets au long de la route A → B pour éviter la fragmentation
  - Émission avec le bit DF = 1 (en-tête IP)
  - Si un routeur doit fragmenter, il retourne à la source un message d'erreur ICMP :



Couche réseau : protocole ARP

Protocole ARP

- *Address Resolution Protocol* (RFC 826)
- Correspondance adresse réseau (IP) → adresse MAC
  - Les applications ne manipulent que des adresses IP
    - Dans un sous-réseau IP : adresses affectées en suivant certaines règles
  - Les trames sont échangées en utilisant les adresses MAC
    - Dans un sous-réseau IP : numérotation aléatoire

Fontionnement d’ARP (1)

- Un ordinateur **A** connecté à un réseau informatique souhaite émettre une trame Ethernet à destination d'un autre ordinateur **B** qui est sur son réseau local et dont il connaît l’adresse IP.
- **A** interroge son cache ARP à la recherche d'une entrée pour **B**

Deux cas peuvent se présenter :

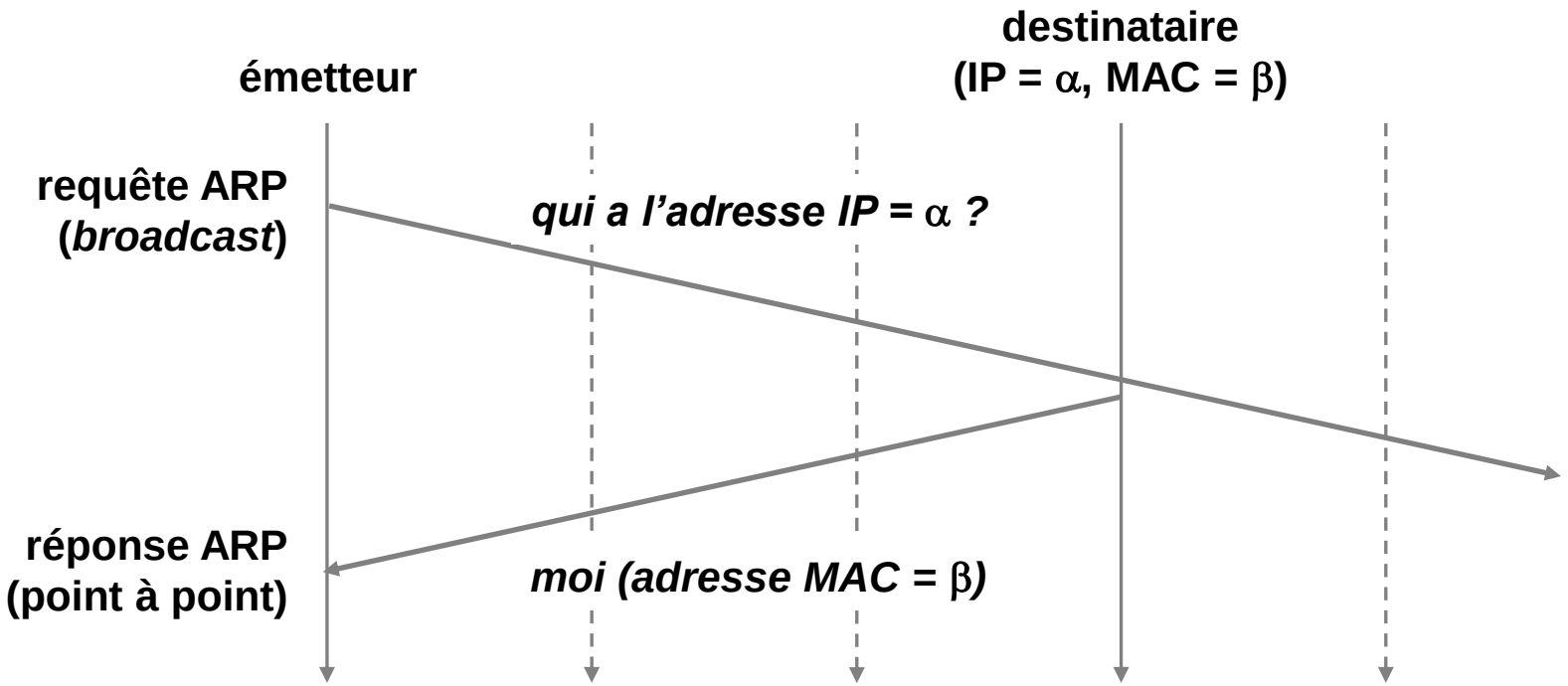
1. L'adresse IP de **B** est présente dans le cache de **A**, il lit l‘adresse MAC correspondante puis envoie la trame Ethernet à **B**.
2. L'adresse IP de **B** est absente. **A** met son émission en attente et effectue une requête ARP en **broadcast**. Cette requête est de type « Quelle est l‘adresse MAC correspondant à l‘adresse IP **@IP_B** ? Répondez à **@MAC_A** ».

Fonctionnement d'ARP (2)

- Tous les ordinateurs connectés au support physique vont recevoir la requête.
- **B** sera le seul ordinateur en envoyant à **A** une réponse ARP du type « je suis @**IP_B**, mon adresse MAC est @**MAC_B** ».
- Pour émettre cette réponse au bon ordinateur, il crée une entrée dans son cache ARP à partir des données qu'il vient de recevoir.
- **A** reçoit la réponse, met à jour son cache ARP et peut donc envoyer le message à **B**.

Protocole ARP (suite)

- Si l'adresse du destinataire n'est pas dans la table ⇒ requête ARP : trame Ethernet en mode diffusion



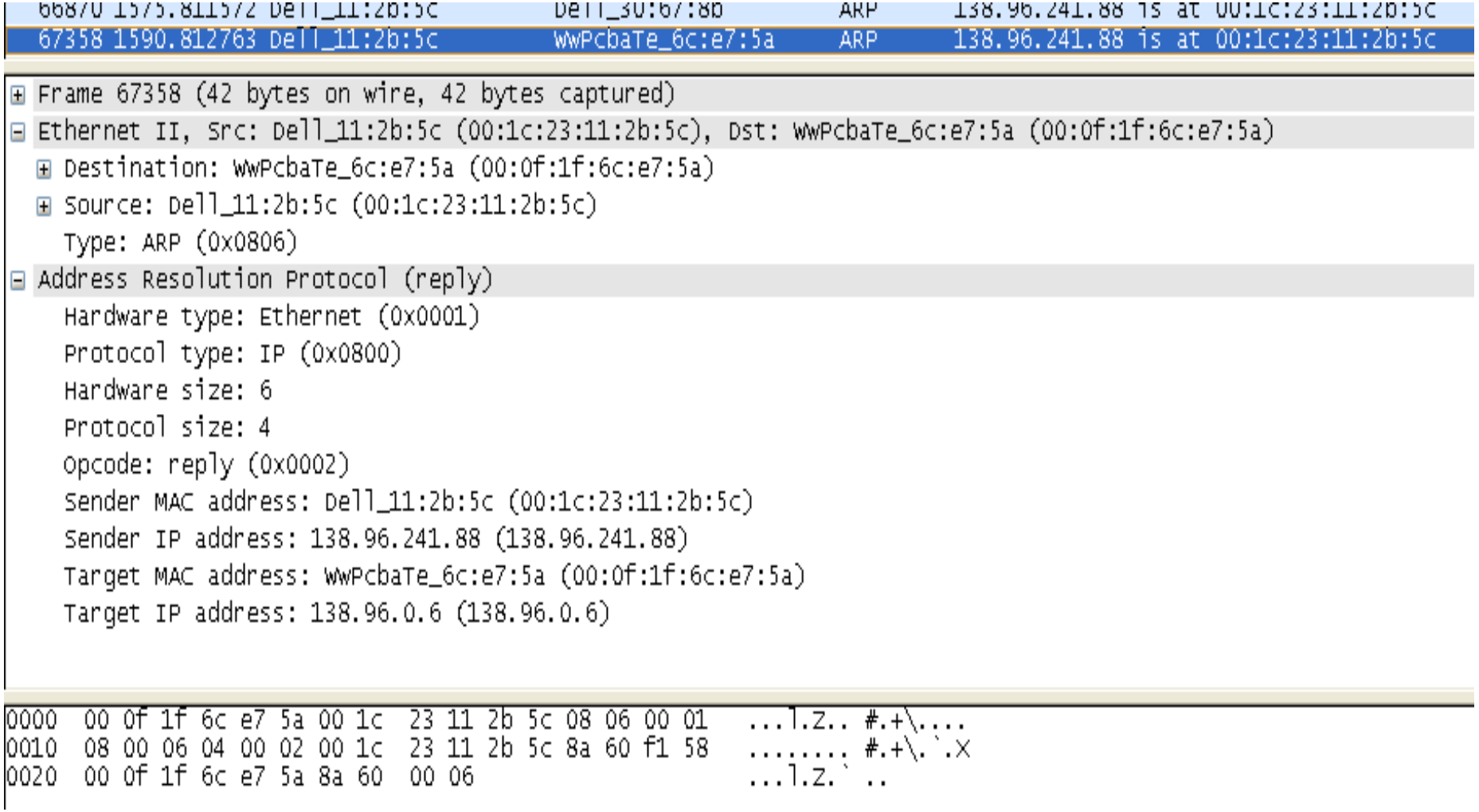
ARP request à tout le monde

```
69753 1656.228884 Dell_79:e0:7b      Broadcast      ARP     Who has 138.96.0.11?  Tell 138.96.215.13
69755 1656.290967 CompaqHp_96:25:a7  Broadcast      ARP     Who has 138.96.93.17?  Tell 138.96.93.23
69756 1656.301907 WwPcbaTe_6d:42:6a  Broadcast      ARP     Who has 138.96.232.79?  Tell 138.96.0.33
69758 1656.377128 Dell_e0:11:b2      Broadcast      ARP     Who has 138.96.211.66?  Tell 138.96.64.23
69759 1656.388077 Cisco_1f:78:0a     Broadcast      ARP     Who has 138.96.43.63?  Tell 138.96.40.250
69760 1656.483019 Intel_de:b0:6a     Broadcast      ARP     Who has 138.96.201.71?  Tell 138.96.160.82
```

```
⊞ Frame 69758 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Dell_e0:11:b2 (00:11:43:e0:11:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Dell_e0:11:b2 (00:11:43:e0:11:b2)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Dell_e0:11:b2 (00:11:43:e0:11:b2)
    Sender IP address: 138.96.64.23 (138.96.64.23)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 138.96.211.66 (138.96.211.66)
```

```
0000  ff ff ff ff ff ff 00 11  43 e0 11 b2 08 06 00 01   ........ C.......
0010  08 00 06 04 00 01 00 11  43 e0 11 b2 8a 60 40 17   ........ C....`@.
0020  00 00 00 00 00 00 8a 60  d3 42 00 00 00 00 00 00   .......` .B......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

ARP reply à celui qui a fait l'ARP request



Structure d’une requête ARP

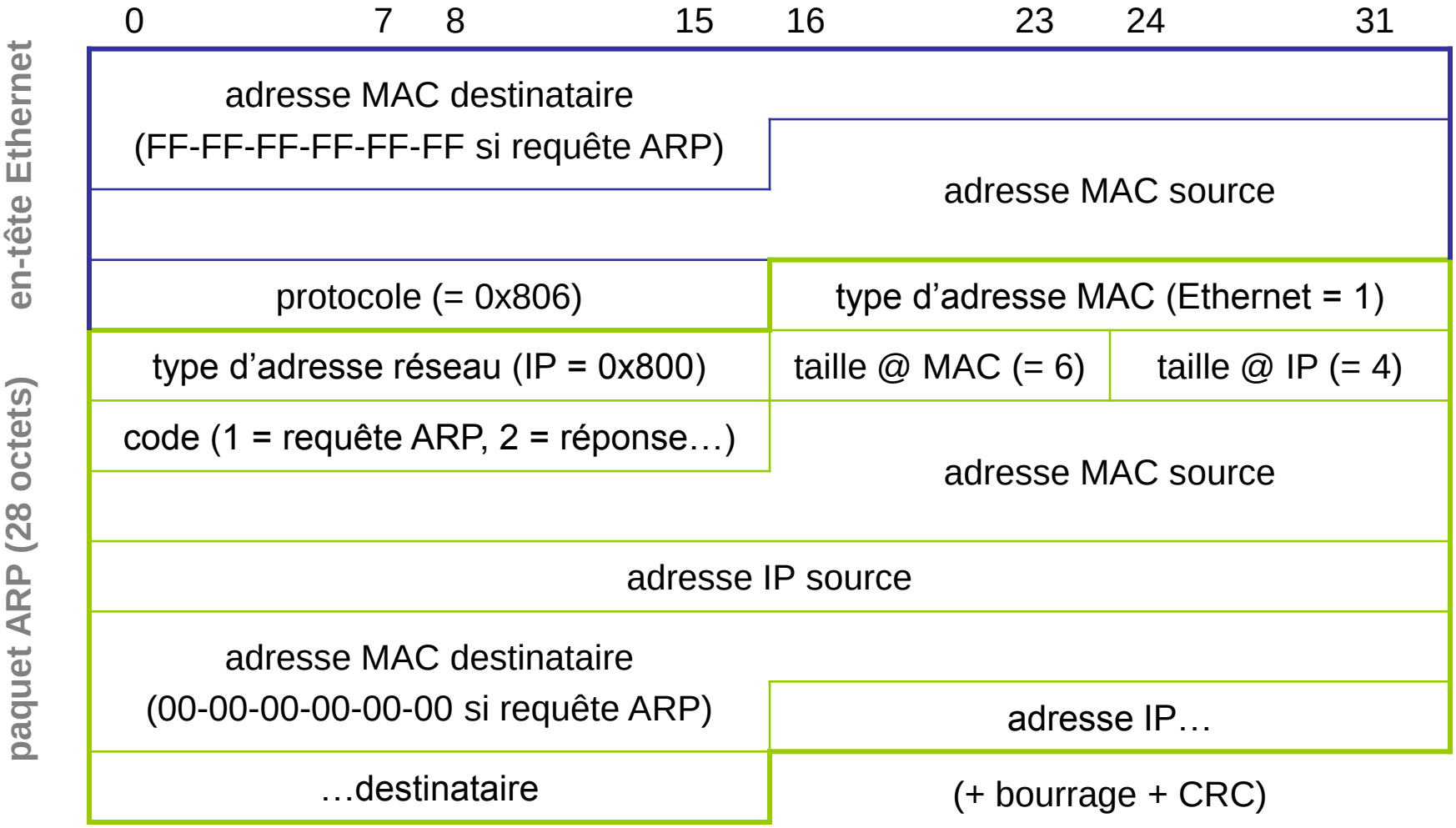
- La requête ARP est véhiculée dans un message protocolaire lui-même encapsulé dans la trame de liaison de données.
- Lorsque la trame arrive à destination, la couche liaison de données détermine l'entité responsable du message encapsulé;
- Champ type de la trame Ethernet : 0X0806 pour ARP

Protocole ARP (suite)

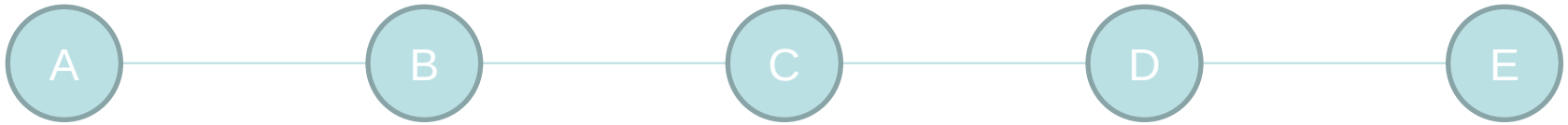
- Table de correspondance (*cache*) dynamique
  - Construite et mise à jour par le système
  - Chaque ligne a une durée de vie finie

```
Z:\>arp -a

Interface : 138.96.241.88 --- 0x2
  Adresse Internet      Adresse physique      Type
  138.96.0.6            00-0f-1f-6c-e7-5a     dynamique
  138.96.0.7            00-11-43-30-67-8b     dynamique
  138.96.0.10           00-0f-1f-6d-42-6a     dynamique
  138.96.0.11           00-0f-1f-6c-e7-5a     dynamique
  138.96.0.23           00-14-22-1e-12-26     dynamique
  138.96.0.33           00-0f-1f-6d-42-6a     dynamique
  138.96.0.34           00-0f-1f-6c-e7-5a     dynamique
  138.96.0.35           00-11-43-30-67-8b     dynamique
  138.96.0.36           00-11-43-30-67-57     dynamique
  138.96.64.10          00-c0-fd-02-0b-1c     dynamique
  138.96.112.250        00-04-de-1f-78-0a     dynamique
  138.96.160.81         00-0c-f1-de-b0-30     dynamique
  138.96.160.82         00-0c-f1-de-b0-6a     dynamique
  138.96.160.83         00-0c-f1-de-a3-6f     dynamique
  138.96.160.84         00-11-11-4d-af-bb     dynamique
  138.96.241.55         00-14-22-1e-03-15     dynamique

Interface : 193.51.208.195 --- 0x3
  Adresse Internet      Adresse physique      Type
  193.51.208.13         00-04-de-1f-78-0a     dynamique
```

Paquet ARP (pour Ethernet et IP)



ARP avec une machine hors de notre réseau local



- Un ordinateur **A** connecté à un réseau informatique souhaite émettre une trame Ethernet à destination d'un autre ordinateur **E** dont il connaît l'adresse IP.
- Pour que la trame atteigne **E**, il faut passer par **B**.
- **A** interroge son cache ARP à la recherche d'une entrée pour **B**

Deux cas peuvent se présenter :

1. L'adresse IP de **B** est présente dans le cache de **A**, il lit l'adresse MAC correspondante puis envoie la trame Ethernet à **E**.
2. L'adresse IP de **B** est absente. **A** met son émission en attente et effectue une requête ARP en **broadcast**. Cette requête est de type « Quelle est l'adresse MAC correspondant à l'adresse IP **@IP_B** ? Répondez à **@MAC_A** ».

ARP avec une machine hors de notre réseau local

- Tous les ordinateurs connectés au support physique vont recevoir la requête.
- **B** sera le seul ordinateur en envoyant à **A** une réponse ARP du type « je suis @**IP_B**, mon adresse MAC est @**MAC_B** ».
- Pour émettre cette réponse au bon ordinateur, il crée une entrée dans son cache ARP à partir des données qu'il vient de recevoir.
- **A** reçoit la réponse, met à jour son cache ARP et peut donc envoyer le message qu'elle avait mis en attente à E en passant par **B**.

Couche Réseau : Adressage

Adressage IPv4

- 32 bits (4 octets). Notation classique : 4 octets en décimal séparés par des ’ . ’
- **Exemple** : 194.214.171.200
- La composition des 32 bits :
  - identification du réseau (net-id)
  - identification de la machine (host-id)
- Taille net-id/host-id : selon la classe de l'adresse.
- Pour garantir l'unicité et le routage, l’**ICANN** (*Internet Corporation for Assigned Names and Numbers)*, est chargée d'attribuer des adresses IP publiques (les adresses IP des ordinateurs directement connectés sur le réseau public internet).
- La partie host-id est assignée par le gestionnaire du réseau local

Allocation des adresses de l'Internet - IANA/ICANN

- Jusqu'en 1998 l'**IANA** (***Internet Assigned Numbers Authority***).
  - alloue l'espace des adresses IP,
  - attribue les identificateurs de protocole (IP)
  - gère le système de nom de domaine de premier niveau et assure les fonctions de gestion du système de serveurs racines

- Ces missions sont désormais assurées par l'**ICANN** (***Internet Corporation for Assigned Names and Numbers***), depuis sa création en 1998.

Allocation des adresses de l'Internet : ICANN/RIR/LIR

- L'ICANN segmente l'espace d'adresses IP en 256 blocs de taille /8, numérotés de 0/8 à 255/8.
- Les adresses IP ***unicast*** sont distribuées aux ***RIR*** (***Registres Internet Régionaux***)
- Les adresses IP sont allouées à l'utilisateur final qui en fait la demande via un ***LIR*** (***Local Internet Registry***), généralement un FAI ou une entreprise multinationale, sous l'autorité de l'instance régionale de gestion de l'adressage.

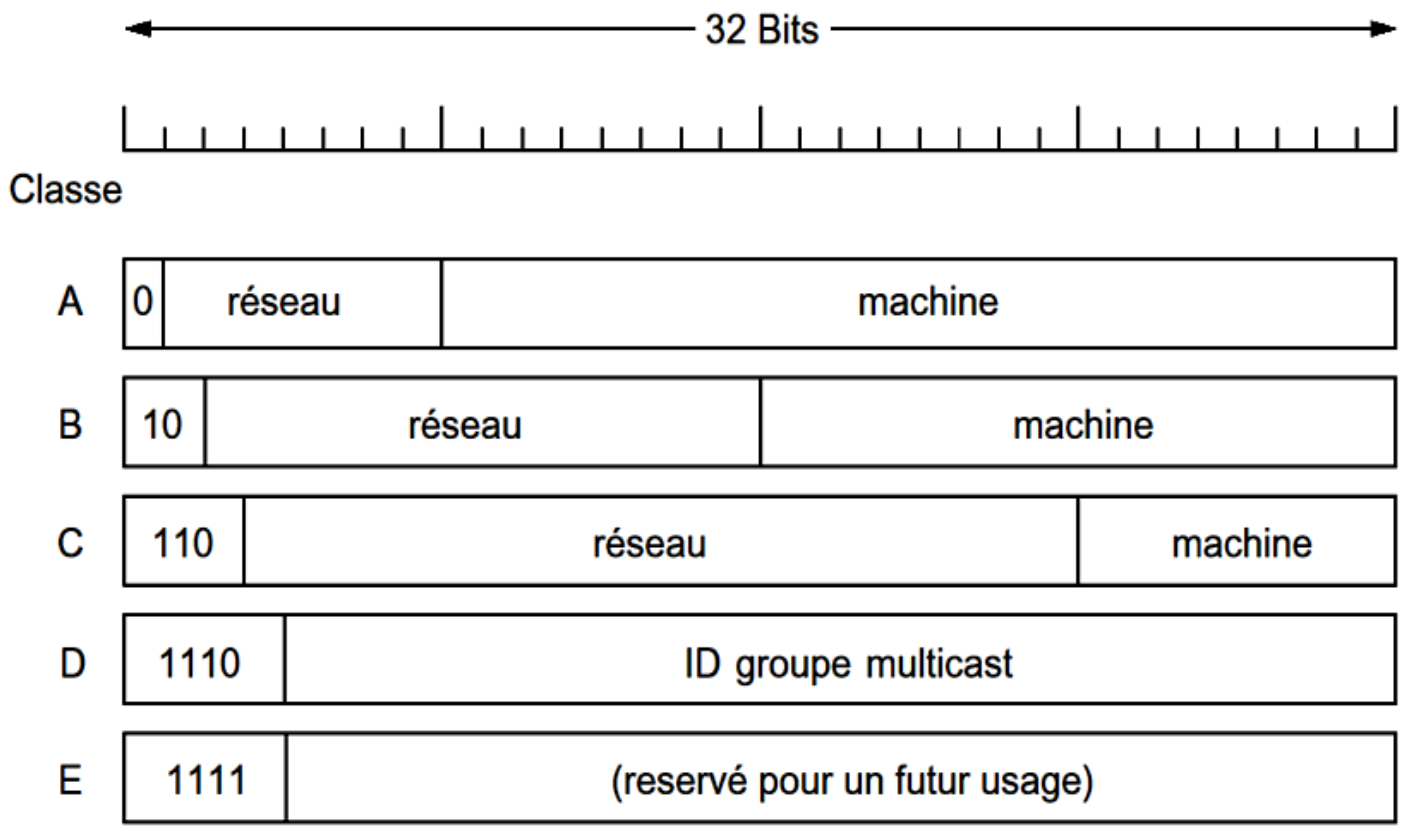
Adresses IP spéciales

- **<net-id><0>** : on obtient **l'adresse réseau**. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.
- **<0><host-id>** : on obtient **l'adresse machine**. Cette adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.
- **<net-id><1>** : on obtient **l'adresse de diffusion** (en anglais **broadcast**). Pour envoyer à toutes les machines situées sur le réseau spécifié par le net- id.
- **<0><0>** : dans les routeurs, route par défaut.
- Enfin, l'adresse **127.0.0.1** désigne la **machine locale** (en anglais **localhost**).

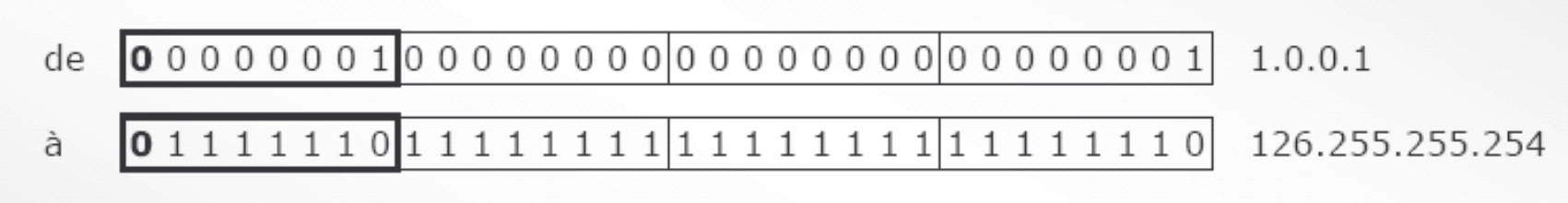
Exemple

- 192.168.1.102 avec masque 255.255.255.0
- Le net-id comporte 24 bits (192.168.1), le host-id en comporte 8 (102).
- Le broadcast = <net-id><1> = ??
- L'adresse réseau = <net-id><0> = ??
- Le nombre de machines sur ce réseau =

Classes d'adresses IP (avant 1994)



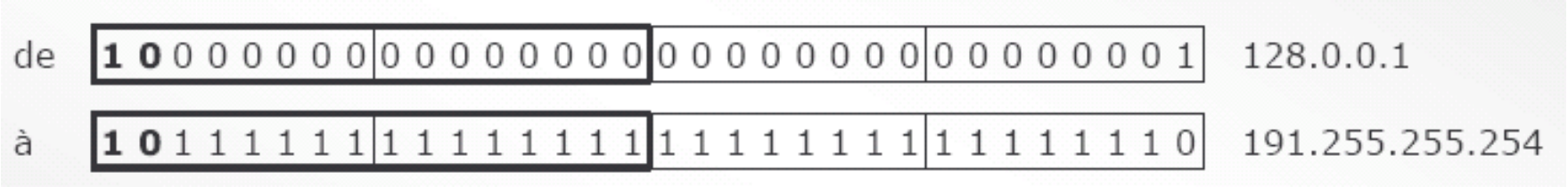
Classe A



De 1.0.0.1 à 126.255.255.254

- net-id = 1er octet
- 1er bit de poids fort à 0
- Adressage de 126 réseaux (2^7-2), chacun pouvant contenir plus de 16 millions (2^{24}-2), de machines.
- Masque = 255.0.0.0

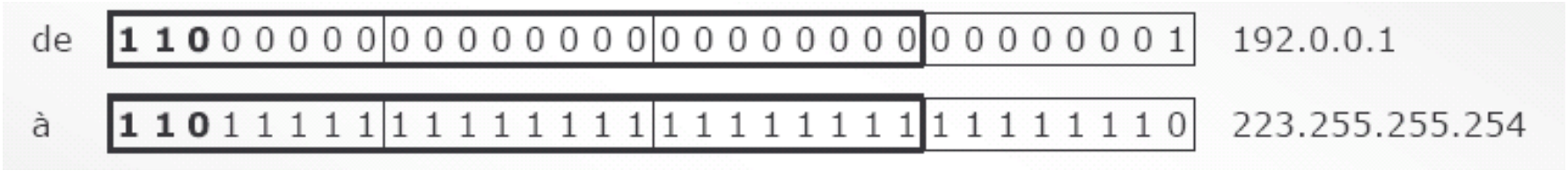
Classe B



De 128.0.0.1 à 191.255.255.254

- net-id = deux premiers octets
- Les 2 bits de poids forts = 10
- Adressage de 16384 réseaux (2^{14}) chacun pouvant contenir 65534 (2^{16}-2) machines
- C'est la classe la plus utilisée, les adresses aujourd'hui sont pratiquement épuisées.
- Masque = 255.255.0.0

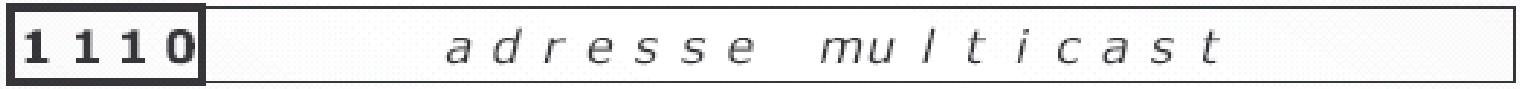
Classe C



De 192.0.0.1 à 223.255.255.254

- net-id = les trois premiers octets, les 3 bits de poids forts sont à 110
- Adressage de plus de 2 millions de réseaux (2^{21}), chacun pouvant contenir 254 machines.
- Masque = 255.255.255.0

Classe D



De 224.0.0.1 à 239.255.255.254

- Les 4 bits de poids forts sont à 1110
- Adresse de diffusion vers les machines d'un même groupe qui se sont abonnées

Adressage IP (avant 1994)

- Espace d'adressage plat
  - Pas de numérotation hiérarchique
  - Pas de rapport entre adresse et localisation géographique : privilégier la simplicité d'administration
- Classes A, B, C : utilisation inefficace et peu flexible des adresses
- Évolutions :
  - CIDR
  - Adresses privées + NAT
  - IPv6 (adresses sur 128 bits)

Couche réseau : CIDR et IPv6

CIDR (Classless Inter-Domain Routing)

- Mis au point afin (principalement) de diminuer la taille de la table de routage contenue dans les routeurs
- Agréger plusieurs entrées de cette table en une seule (par région géographique et fournisseurs d'accès)
- Agrégation maximum des sous-réseaux qui sont routés ensembles avec la même politique
- L'adresse IP est suivie par un slash ("/") indiquant le nombre de bits correspondant au net-id

- **Exemple :** 192.0.2.96/23 indique une adresse IP où les 23 premiers bits sont utilisés comme adresse réseau.

Le masque comporte 23 '1' suivis de 9 '0': 255.255.254.0

Rappel : 1111 1111 = 255

192.168.1.3/24, |net-id|=24

- **Masque =** 11111111.11111111.11111111.00000000
  24 ‘1’ et 8 ‘0’ = 255.255.255.0
- **@réseau** = 192.168.1.0
  24 bits du net-id suivis de 8 ‘0’
- **@broadcast** = 192.168.1.255
  24 bits du net-id suivi de 8 ‘1’

- **Nombre de machines** = 2^8-2 = 254 ($2^{|\text{host-id}|}$ - 2)
- **Plage d’adresses** = de 192.168.1.1 à 192.168.1.254 (on enlève le broadcast et l’adresse réseau)

134.59.1.3/16, |net-id|=??

- **Masque =** ??
- **@réseau** =??
- **@broadcast** = ??
- **Nombre de machines** =??
- **Plage d’adresses** = ??

134.59.1.3/16, |net-id|=16

- **Masque =** 11111111.11111111.00000000.00000000
  = 255.255.0.0
- **@réseau** = **134.59**.0.0
- **@broadcast** = **134.59**.255.255
- **Nombre de machines** = 2^{16}-2 = 65534 ($2^{|\text{host-id}|}$ - 2)
- **Plage d'adresses** = de 134.59.0.1 à 134.59.255.254

Exemple : 192.44.77.0 /26

- **MASQUE :** 26 ‘un’ suivis de 6 ‘zéro’ (8 ‘un’ = 255)
  - **255.255.255.11**000000 = 255.255.255.192
- **ADRESSE RESEAU :** je recopie les 26 bits de l’adresse, je complète par des ‘zéro’
  - **192.44.77.00**000000 = 192.44.77.0
- **BROADCAST :** je recopie les 26 bits de l’adresse, je complète par des ‘un’
  - **192.44.77.00**111111 = 192.44.77.63
- **NOMBRE DE MACHINES :** $2^{|host\text{-}id|} - 2$
  - $2^6 – 2 = 62$
- **PLAGE D’ADRESSES :** De ‘@réseau +1’ à ‘@Broadcast -1’
  - De 192.44.77.1 à 192.44.77.62

Subnetting

- Diviser un **gros réseau** unitaire en ce qui apparaît comme **plusieurs sous-réseaux**

- Les sous-réseaux sont utiles pour réduire le nombre d'entrées dans la table de routage pour Internet en cachant des informations sur les sous-réseaux individuels d'un site

- De plus, cela a permis de réduire la surcharge réseau (overhead), en divisant le nombre d'hôtes recevant des appels broadcast IP

Subnetting

- **Masque de sous-réseau :** indique le nombre de bits utilisés pour identifier le sous-réseau, et le nombre de bits caractérisant les hôtes.
- Un masque de sous réseau est une adresse de 32 bits contenant des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut rendre égaux à zéro.
- Une fois ce masque créé, il suffit de faire un ET entre la valeur que l'on désire masquer et le masque afin de garder intacte la partie que l'on désire et annuler le reste
- Il y a plusieurs avantages à utiliser ce procédé. Un d'entre eux est de pouvoir connaître le réseau associé à une adresse IP.

Exemple de masque de sous-réseau

Exemple : 130.79.153.28/23

Ecriture binaire

Adresse : 10000010 01001111 10011001 00011100

Masque : 11111111 11111111 11111110 00000000

On fait un **ET** logique

Adresse réseau : 10000010 01001111 10011000 00000000

En décimal : 130.79.152.0

1. Est-ce que l'adresse 130.79.154.1 fait partie de ce réseau ?
2. Et l'adresse 130.79.153.35 ?

Exemple de création de sous-réseaux

- 130.79.153.28/23 : adresse réseau 130.79.152.0
- Adresse réseau : 10000010 01001111 1001100**0** 00000000
- Si je veux créer 3 sous-réseaux : j'ai besoin de 2 bits supplémentaires dans l'adresse réseau pour les créer (je crée ainsi 4 sous-réseaux).
  1. 10000010 01001111 1001100**0 0**0000000 : 130.79.152.0/25
  2. 10000010 01001111 1001100**0 1**0000000 : 130.79.152.128/25
  3. 10000010 01001111 1001100**1 0**0000000 : 130.79.153.0/25
  4. 10000010 01001111 1001100**1 1**0000000 : 130.79.153.128/25

- Chaque sous-réseau pourra adresser 126 hôtes.

Exemple Salles 6** au Dept. INFO

VLAN	@reseau	Masque	Passerelle
651	134.59.27.32/27	255.255.255.224	134.59.27.62
655	134.59.27.64/27	255.255.255.224	134.59.27.94
659	134.59.27.96/27	255.255.255.224	134.59.27.126
663	134.59.27.128/27	255.255.255.224	134.59.27.158
665	134.59.27.160/27	255.255.255.224	134.59.27.190

Attribution d'adresses IP

- On distingue 2 méthodes d'attribution des adresses IP pour les hôtes :
  - **Statique :** chaque équipement est configuré avec une adresse unique
  - **Dynamique :** on utilise des protocoles qui attribue dynamiquement les adresses IP dès la connexion à partir d'un pool d'adresses.

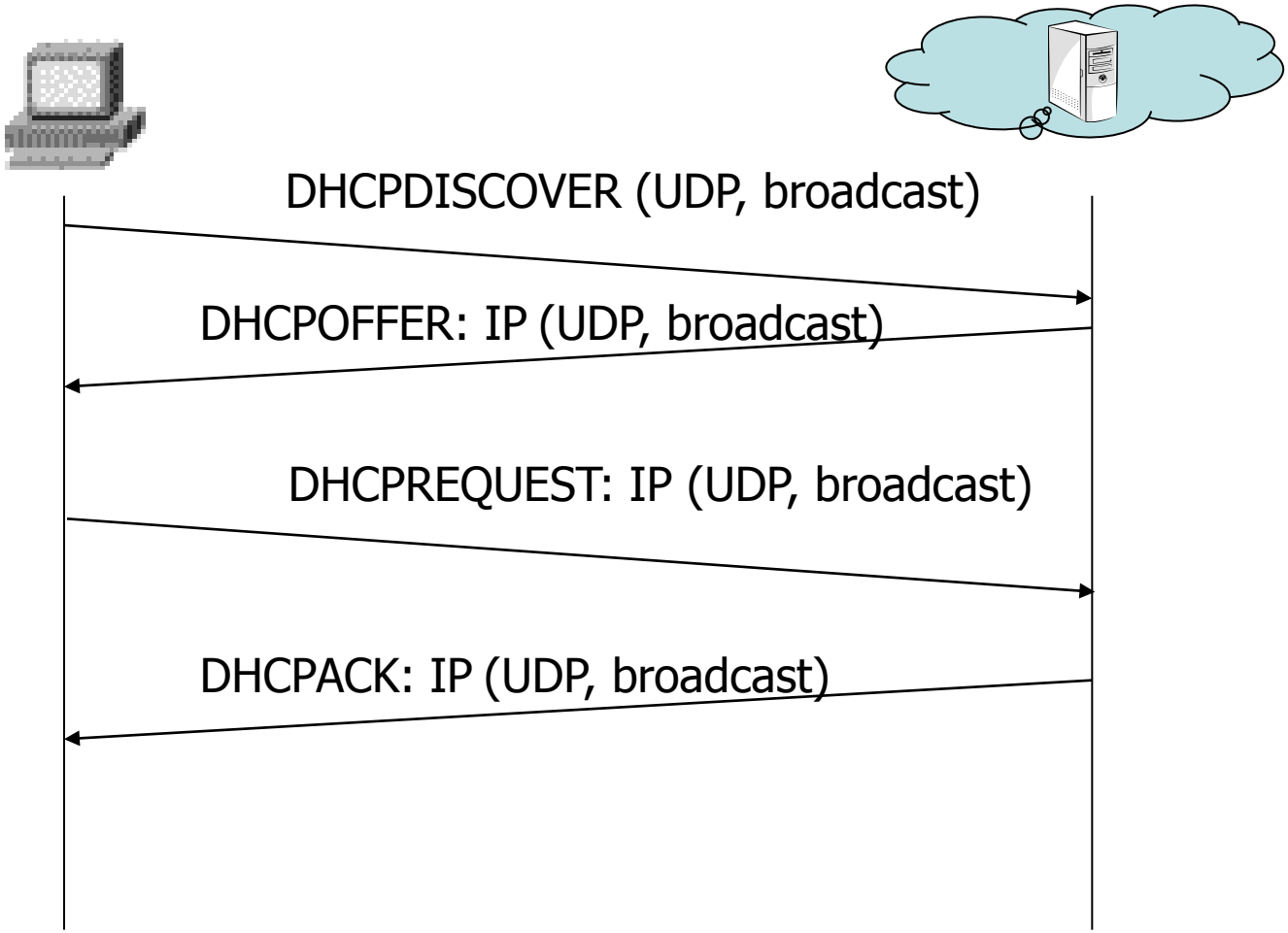
Attribution d'adresses IP

- Pour l'attribution dynamique des adresses IP, on utilise des protocoles qui attribuent des IP aux hôtes :
  - **BOOTP :** Ce protocole permet à un équipement de récupérer son adresse IP au démarrage. L'émetteur envoi un message de broadcast (255.255.255.255) reçu par le serveur qui répond lui aussi par un broadcast contenant l'adresse MAC de l'émetteur ainsi qu'une IP.
  - **DHCP :** Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et l'attribue à l'hôte. Avec le protocole DHCP, il est également possible pour un ordinateur de récupérer sa configuration complète (adresse, masque de sous réseau, etc.)

DHCP *(Dynamic Host Configuration Protocol)*

- Pour connecter une machine à l'Internet, DHCP configure dynamiquement :
  1. Une adresse IP unique dans le réseau local et appartenant au même réseau logique que toutes les autres machines du réseau,
  2. L'adresse IP d'une passerelle qui permet d'accéder à l'extérieur,
  3. L'adresse IP d'un serveur DNS pour pouvoir résoudre les noms des hôtes,
  4. un masque de sous réseau, le même pour tous les hôtes du réseau.

Modèle de fonctionnement



Messages DHCP

- DHCPDISCOVER : localiser les serveurs DHCP disponibles
- DHCPOFFER : réponse du serveur à un paquet DHCPDISCOVER, contenant les premiers paramètres
- DHCPREQUEST : requête diverse du client pour, par exemple, prolonger son bail
- DHCPACK : réponse du serveur qui contient des paramètres et l'adresse IP du client
- DHCPNAK : réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau
- DHCPDECLINE : le client annonce au serveur que l'adresse est déjà utilisée
- DHCPRELEASE : le client libère son adresse IP
- DHCPINFORM : le client demande des paramètres locaux

Couche réseau : routage

Routage

- Le principe de base du routage est synthétisé par les deux étapes suivantes :
  - **Détermination du chemin :** table de routage pour déterminer quel est le meilleur chemin à emprunter pour atteindre la destination. Les métriques utilisées afin d'offrir une mesure de qualité pour un chemin.
  - **Commutation :** permet à un routeur d'accepter un paquet d'une interface et de le transmettre par le biais d'une autre interface. Le paquet pris en charge à une interface est retransmis via une autre interface représentant le meilleur chemin vers la destination.

Tables de routage

- Trouver une route pour atteindre une adresse machine donnée
- Localement : sur quelle interface, et éventuellement avec quelle adresse MAC un paquet doit-il être (re)transmis encapsulé dans une trame ?
- Décision : prise à l'aide d'info locales disponibles dans une table de routage
- **Deux aspects :**
  - utiliser de proche en proche des tables de routage pour tracer une route
  - créer et mettre à jour les tables de routage

Que fait un routeur quand il reçoit un datagramme IP ?

- Vérifie le checksum. Si faux, destruction du datagramme.
- Décrémente le TTL.
- Décide du routage (prochain saut) en regardant la table de routage.
- Fragmente le datagramme si nécessaire.
- Reconstruit l'entête IP avec les champs mis à jour.
- Modifie l'entête de niveau 2
- Retransmet les datagrammes au protocole d'accès de l'interface réseau de sortie avec l'adresse de sous-réseau correspondante

Les tables de routage

- Les tables de routage contiennent trois informations :
  - **Destination :** réseau, sous-réseau, machine, default (0.0.0.0)
  - **Chemin :** interface locale à la machine, un routeur intermédiaire
  - **Coût ou métrique :** nombre de hops, débit

- Le **et bits à bits** entre l'adresse à router et le masque doit être égal à l'adresse destination pour que l'entrée de la table soit candidate.

Exemple d'une table de routage

Réseau	Masque	Moyen de l'atteindre
192.168.2.0	255.255.255.0	eth0
100.0.0.0	255.0.0.0	eth1
101.0.0.0	255.0.0.0	eth2
192.168.1.0	255.255.255.0	100.0.0.1
192.168.3.0	255.255.255.0	101.0.0.2

route print

```
Z:\>route print
===========================================================================
Liste d'Interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 1c 23 11 2b 5c ...... Broadcom NetXtreme 57xx Gigabit Controller #5 -
Miniport d'ordonnancement de paquets
0x3 ...00 1b 77 c8 1c fe ...... Intel(R) PRO/Wireless 3945ABG Network Connection
 #2 - Miniport d'ordonnancement de paquets
===========================================================================
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0   138.96.112.250   138.96.241.88       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
       138.96.0.0      255.255.0.0    138.96.241.88   138.96.241.88       20
    138.96.241.88  255.255.255.255        127.0.0.1       127.0.0.1       20
   138.96.255.255  255.255.255.255    138.96.241.88   138.96.241.88       20
        224.0.0.0        240.0.0.0    138.96.241.88   138.96.241.88       20
  255.255.255.255  255.255.255.255    138.96.241.88                3        1
  255.255.255.255  255.255.255.255    138.96.241.88   138.96.241.88       1
Passerelle par défaut :    138.96.112.250
===========================================================================
Itinéraires persistants :
  Aucun
```

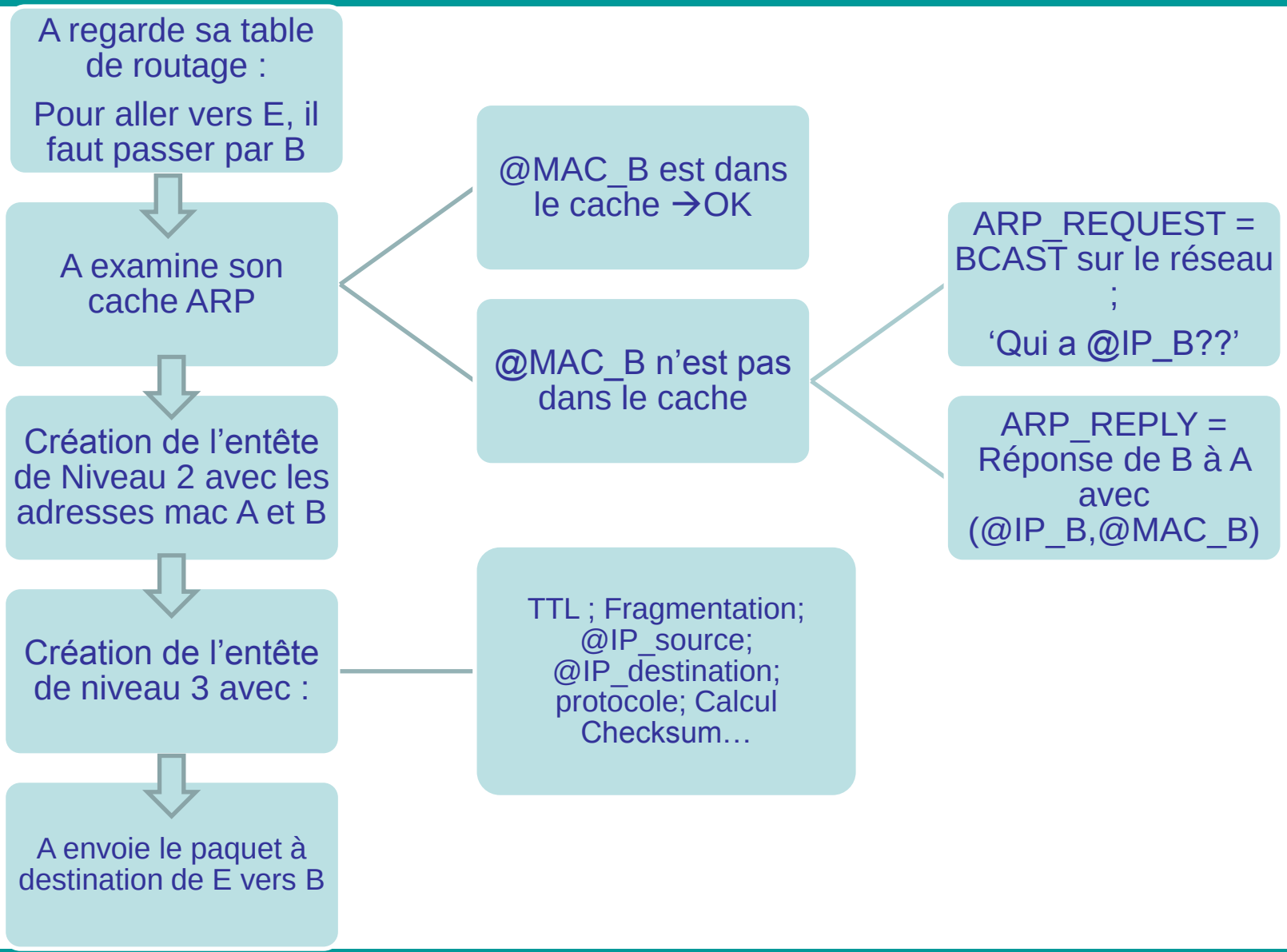
Examen de la table de routage

- Le routeur examine l'adresse destination du paquet.
  1. Si la destination est sur le même réseau physique : **routage direct**. L'adresse physique suivante est celle de la destination, le paquet est transmis directement.
  2. Sinon, si la destination correspond à celui d'un réseau accessible via un routeur on récupère l'adresse physique de ce routeur et on lui transmet le paquet : **routage indirect**. L'adresse IP de l'émetteur reste inchangée.
  3. Si le préfixe n'a pas de correspondance dans la table mais il existe un routeur par défaut dans la table ; on transmet au routeur par défaut.
  4. Si aucun des trois cas précédents n'est rempli, on déclare une erreur de routage.

A envoie un ping à E

- A examine sa table de routage pour déterminer le prochain saut pour aller vers E → il s'agit de B
- A examine le cache ARP et éventuellement requête ARP sur le réseau local pour récupérer l'@mac de B
- Construction de toutes les entêtes nécessaires et envoi du paquet vers le prochain saut

A envoie un ping à E



A envoie un ping à E

ICMP Echo Request (Type = 8; code = 0)
Source = @IP_A; Destination = @IP_E; TTL = 128 ; protocole = ICMP; Checksum;
@MAC_SRC = MAC_A; @MAC_DST = MAC_B; type = IPv4;

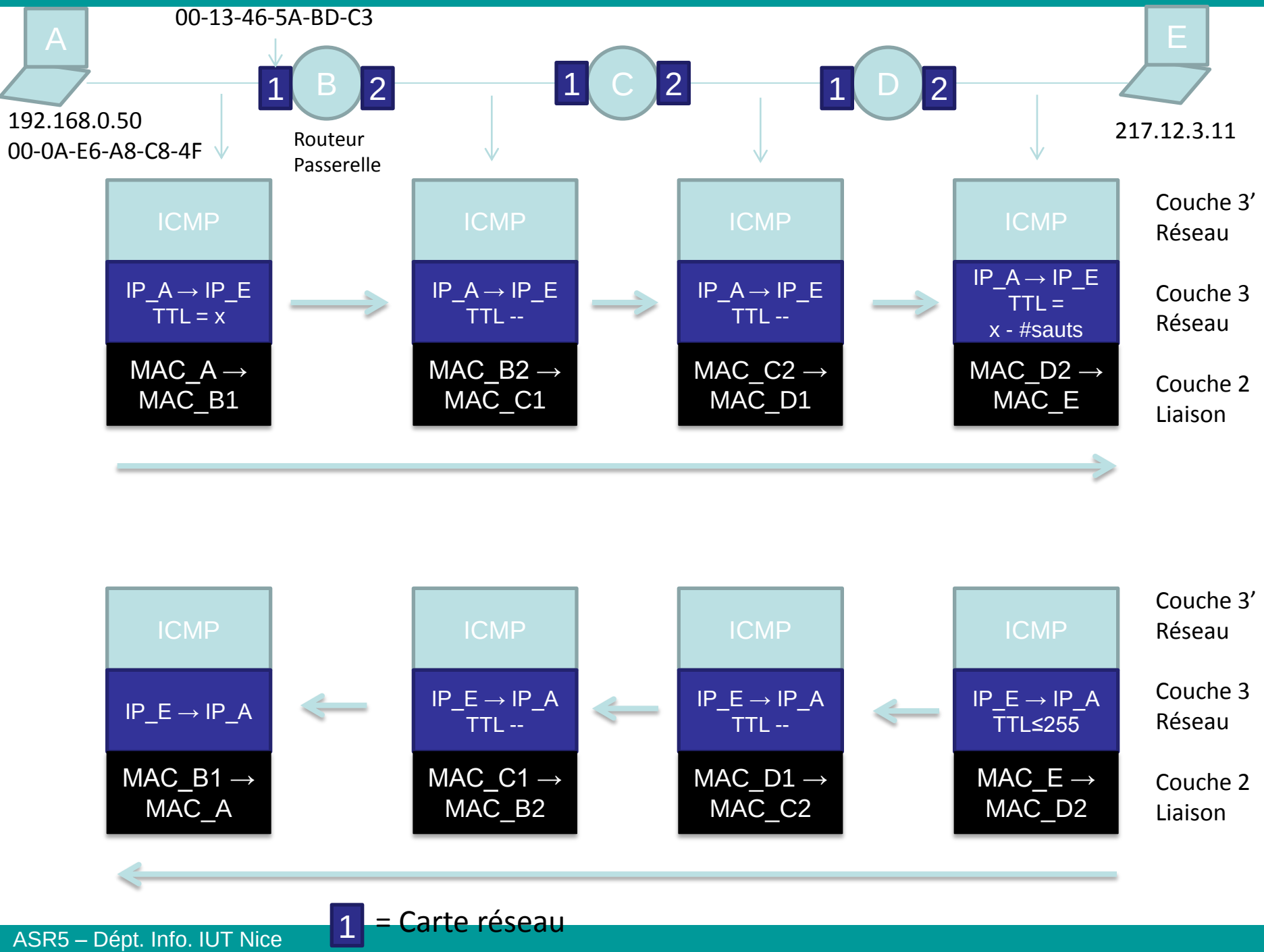
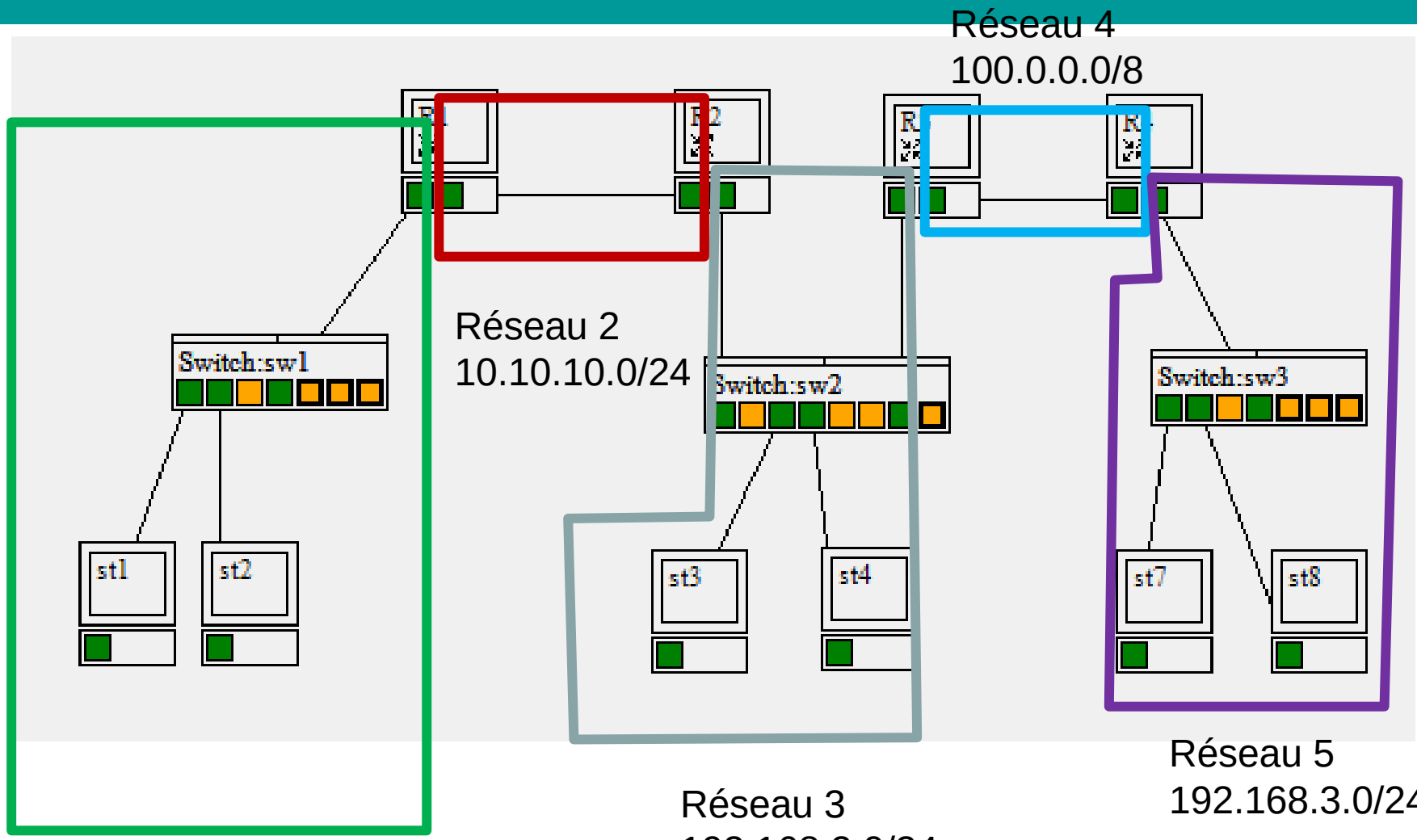

A
00-13-46-5A-BD-C3
B
1
2
C
1
2
D
1
2
E
192.168.0.50
00-0A-E6-A8-C8-4F
Routeur
Passerelle
217.12.3.11
ICMP
IP_A → IP_E
TTL = x
MAC_A → MAC_B1
ICMP
IP_A → IP_E
TTL --
MAC_B2 → MAC_C1
ICMP
IP_A → IP_E
TTL --
MAC_C2 → MAC_D1
ICMP
IP_A → IP_E
TTL =
x - #sauts
MAC_D2 → MAC_E
Couche 3' Réseau
Couche 3 Réseau
Couche 2 Liaison
ICMP
IP_E → IP_A
MAC_B1 → MAC_A
ICMP
IP_E → IP_A
TTL --
MAC_C1 → MAC_B2
ICMP
IP_E → IP_A
TTL --
MAC_D1 → MAC_C2
ICMP
IP_E → IP_A
TTL≤255
MAC_E → MAC_D2
Couche 3' Réseau
Couche 3 Réseau
Couche 2 Liaison
1 = Carte réseau

Table de routage de R1?



DNS - Domain Name Server

- Annuaire permettant d'associer des noms à des adresses IP.
  - www.free.fr en 212.27.48.10
  - www.google.com en 209.85.137.99
  - ….
- Il est plus facile de se rappeler du nom que de l'adresse IP…
- et inversement : résolution inverse

Organisation Hiérarchique

- L'espace de noms est organisé en une hiérarchie au sommet de laquelle se trouve la racine et immédiatement en dessous les TLD (Top-Level Domain) ou domaines de niveau supérieur.
- L'ICANN (Internet Corporation for Assigned Names and Numbers) a en charge la création des TLD :
  - com : entreprises commerciales
  - edu : etablissements d'enseignement
  - org : organisations diverses
- un TLD par code pays sur 2 lettres (norme ISO 3166) :
  - Fr : France
  - uk : Royaume-Uni
  - de : Allemagne

13 serveurs racines

Lettre	adresse IPv4	adresse IPv6	Société	Sites (global/local)
A	198.41.0.4	2001:503:ba3e::2:30	VeriSign	6 (6/0)
B	192.228.79.201	2001:478:65::53 (pas encore dans la zone)	USC-ISI (en)	1 (1/0)
C	192.33.4.12	2001:500:2::c (pas encore dans la zone)	Cogent Communications	6 (6/0)
D	199.7.91.13	2001:500:2d::d	Université du Maryland	1 (1/0)
E	192.203.230.10		NASA	1 (1/0)
F	192.5.5.241	2001:500:2f::f	Internet Systems Consortium	49 (2/47)
G	192.112.36.4		Defense Information Systems Agency (en)	6 (6/0)
H	128.63.2.53	2001:500:1::803f:235	United States Army Research Laboratory (en)	1 (1/0)
I	192.36.148.17	2001:7fe::53	Autonomica	36
J	192.58.128.30	2001:503:c27::2:30	VeriSign	70 (63/7)
K	193.0.14.129	2001:7fd::1	RIPE NCC	18 (5/13)
L	199.7.83.42	2001:500:3::42	ICANN	38 (37/1)
M	202.12.27.33	2001:dc3::35	WIDE Project	6 (5/1)

- Les informations sur les domaines sont accessibles via des serveurs de noms, on dit qu'un serveur a l'autorité sur une certaine information si celle-ci est contenue dans son fichier zone.
- Redondance de l'information grâce à l'utilisation de serveurs maîtres primaires et secondaires (ou encore esclaves) avec les mêmes données sur la zone et le même niveau d'autorité sur l'information que les serveurs primaires.

Serveurs primaires/secondaires

- Le serveur maître primaire met à jour ses informations de zone localement par la modification "en dur "de son fichier zone (intervention humaine), alors que
- Le serveur maître secondaire obtient les mises à jour du fichier zone via une opération que l’on nomme transfert de zone. Il contacte donc régulièrement un serveur primaire et vérifie si son fichier zone est à jour, sinon il le télécharge sans intervention humaine

Informations d'une base DNS

- A : Adresse IPv4 d'ordinateur
- AAAA : Adresse IPv6 d'ordinateur
- MX : (Mail eXchanger) adresse du serveur SMTP du domaine.
- CNAME : nom canonique pour un alias (autre nom pour le domaine)
- NS : (Name Server) nom d'un serveur de noms du domaine
- PTR : lien vers un autre nom de domaine. Utilisée surtout pour la résolution inverse
- SOA : (Start Of Authority) plusieurs paramètres concernant le domaine :
  - nom du serveur primaire de la zone
  - adresse mail du responsable, où @ est remplacée par . (point)
  - durée de vie (TTL) des enregistrements fournis

nslookup

```
C:\Users\jmoulier>nslookup www.google.fr
Serveur :    dns1.proxad.net
Address:  212.27.40.240

Réponse ne faisant pas autorité :
Nom :    www.google.fr
Addresses:  2a00:1450:400c:c05::5e
          173.194.67.94


C:\Users\jmoulier>
```

IPv6

Iana.org – *Address Space registry*

- **Exemples d'allocation de /8 avant 1994**

IANA IPv4 Address Space Registry

Last Updated
2011-02-03
Description
The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world. RFC 1466 [RFC1466] documents most of these allocations.

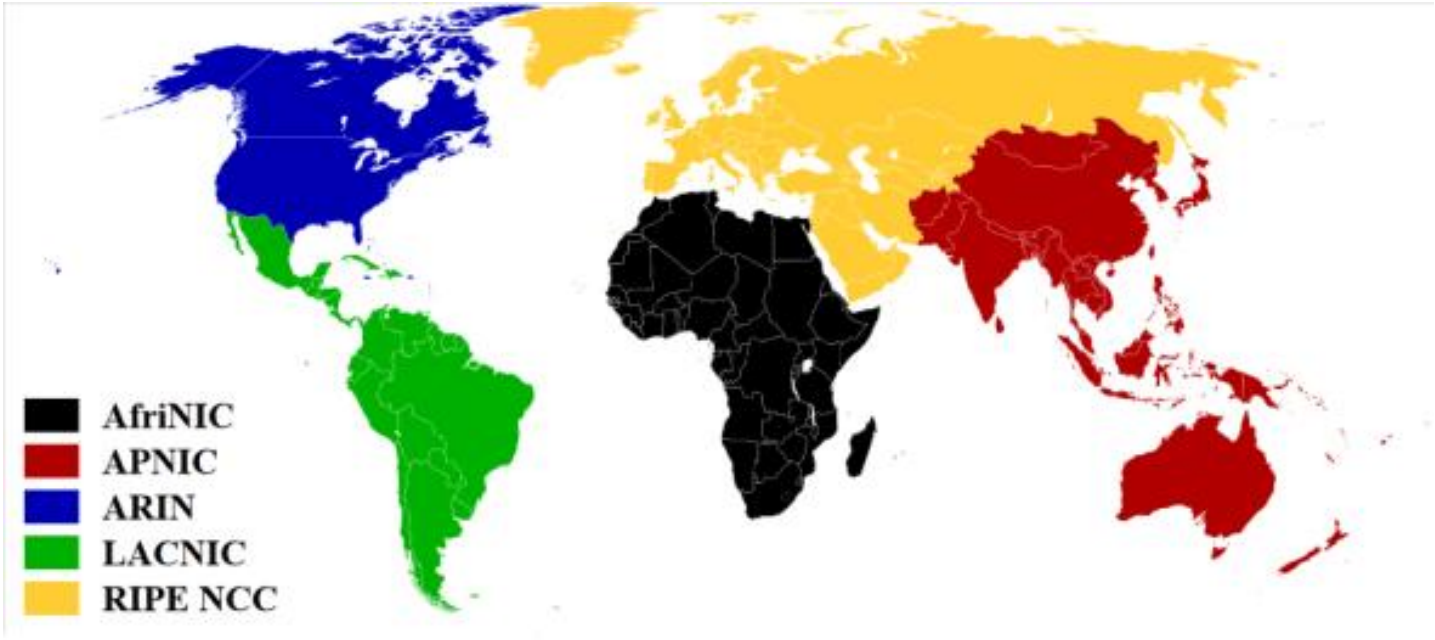
This registry is also available in plain text.

Prefix	Designation	Date	Whois	Status [1]	Note
000/8	IANA - Local Identification	1981-09		RESERVED	[2]
001/8	APNIC	2010-01	whois.apnic.net	ALLOCATED	
002/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED	
003/8	General Electric Company	1994-05		LEGACY	
004/8	Level 3 Communications, Inc.	1992-12		LEGACY	
005/8	RIPE NCC	2010-11	whois.ripe.net	ALLOCATED	
006/8	Army Information Systems Center	1994-02		LEGACY	
007/8	Administered by ARIN	1995-04	whois.arin.net	LEGACY	
008/8	Level 3 Communications, Inc.	1992-12		LEGACY	
009/8	IBM	1992-08		LEGACY	
010/8	IANA - Private Use	1995-06		RESERVED	[3]
011/8	DoD Intel Information Systems	1993-05		LEGACY	
012/8	AT&T Bell Laboratories	1995-06		LEGACY	
013/8	Xerox Corporation	1991-09		LEGACY	
014/8	APNIC	2010-04	whois.apnic.net	ALLOCATED	[4]

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

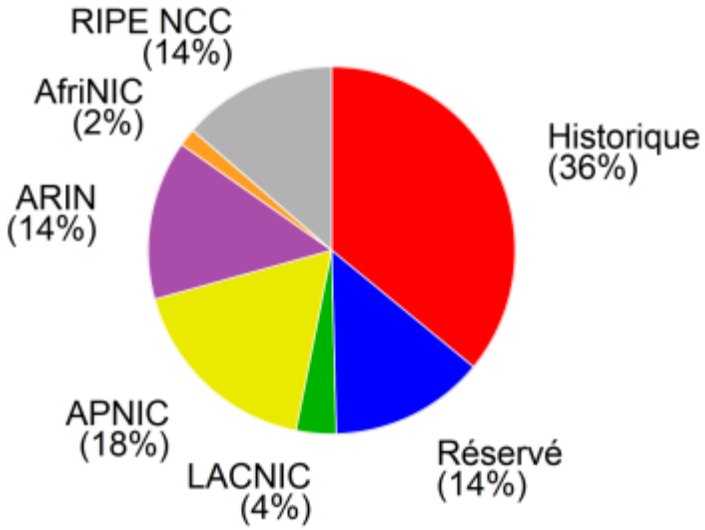
Allocation des adresses de l'Internet : ICANN/RIR/LIR

- Les adresses IP ***unicast*** sont distribuées aux ***RIR*** (***Registres Internet Régionaux***)



- Les adresses IP sont allouées à l'utilisateur final qui en fait la demande via un ***LIR*** (***Local Internet Registry***), généralement un FAI ou une entreprise multinationale, sous l'autorité de l'instance régionale de gestion de l'adressage.

Etat Courant de l'allocation IPv4



- **Le 3 février 2011, l'IANA a annoncé que les cinq derniers blocs /8 libres ont été attribués aux 5 RIR.**
- L'IANA prévoit que les RIR commenceront à manquer d'adresses disponibles à assigner aux LIR au cours de l'année **2011**, et que certains LIR ne seront plus en mesure d'attribuer de nouvelles adresses IPv4 au cours de l'été **2012**.
- **Le 14 Avril 2011, l'APNIC atteint le seuil critique de 1 unique /8 et restreint les allocations à 1024 adresses. RIPE NCC devrait prochainement suivre …**

Historique d'IPv6 – Les dates charnières

- **1990** : Détection du problème de l'épuisement prévisible d'adresses IPv4 (fin de l'Internet prévue 1994!)
- **1992** : Démarrage de l'activité commerciale (qui amplifie le problème), Premières mesures, notamment CIDR
- **1992** : ***IPng Working Group***
- **1993** : Durcissement de la politique d'allocation, définition des adresses privées (fin de l'Internet repoussée en 2008)
- **1994** : Premier standard IPv6 (taille des adresses, format du paquet)
- **1995** : ***RFC1883*** « *Internet Protocol, Version 6 (IPv6) Specification* »
- **1996** : Démarrage du réseau d'expérimentation 6bone qui s'étend en Asie, Europe , Amérique et Australie.
- **1996** : ***IPng Working Group*** devient ***IPv6 Working group***
- **1998** : ***RFC2460*** « *Internet Protocol, Version 6 (IPv6) Specification* »
- **1999** : L'activité de standardisation se porte sur les problèmes de migration et cohabitation IPv4 / IPv6
- **2001** : Début de la distribution d'adresses IPv6 officielles
- **2003** : Création de l'***IPv6Ready Logo Program***, programme mondial de certification IPv6

Les améliorations du Protocole IPv6

- IPv6 apporte un certain nombre de nouvelles fonctionnalités par rapport à IPv4 :
  - Un plus grand espace d'adressage ,
  - Un entête simplifié et efficace
  - Le support de la mobilité
  - La sécurité de bout en bout
  - l'autoconfiguration des machines sans état,
  - des adresses locales pour les liens,
  - pas de fragmentation des paquets, et plus de somme de contrôle,
  - Suppression du NAT.

Adresses IPv6

- Les adresses IPv6 sont codées sur ***128bits***, pour IPv4 on a 32bits.
  - ⇒ 4 294 967 296 de machines pour IPv4
  - ⇒ 3,40282366920938463463374607431768e+38 pour IPv6 (plus de 667 millions de milliards d'adresses par millimètre carré de surface terrestre)

- Elles sont ***découpées en 8 mots de 16 bits*** (4 chiffres hexadécimaux) ***séparés par des « : ».*** En comparaison les adresses IPv4 sont constituées de 4 octets, chaque octet étant noté par sa forme décimale; les différents octets étant séparés par des « **.** »

- **Exemples** :
  - fe80:0000:0000:0000:0240:96ff:fea7:00d3
  - 2001:0c28:0000:8523:0000:0000:ac2f:b2b3

Adresses IPv6 : Simplification d'écriture

- La notation pouvant être fastidieuse, les méthodes de simplification suivantes ont été définies :
  - **La notation « :: » permet de représenter plusieurs 0 consécutifs au sein de plusieurs mots de 16 bits**. Le nombre de 0 peut être retrouvé en examinant le nombre de mots présents dans l'adresse. Cet élément ne peut être présent qu'une fois au sein de l'adresse,
  - **Au sein d'un mot de 16 bits les chiffres hexadécimaux de poids fort positionnés à 0 peuvent être omis.**

Exemple : fe80:0000:0000:0000:0240:96ff:fea7:00d3

- simplification 1 => fe80::0240:96ff:fea7:00d3
- simplification 2 => fe80::240:96ff:fea7:d3

Question / Simplification d'écriture

Simplifier l'écriture :

3FFE:0000:0F0F:0000:0000:0000:00A0:1200

Réponse / Simplification d'écriture

3FFE:0000:0F0F:0000:0000:0000:00A0:1200

3FFE:**0000**:**0**F0F:**0000:0000:0000**:**00**A0:1200

Simplification 1 :

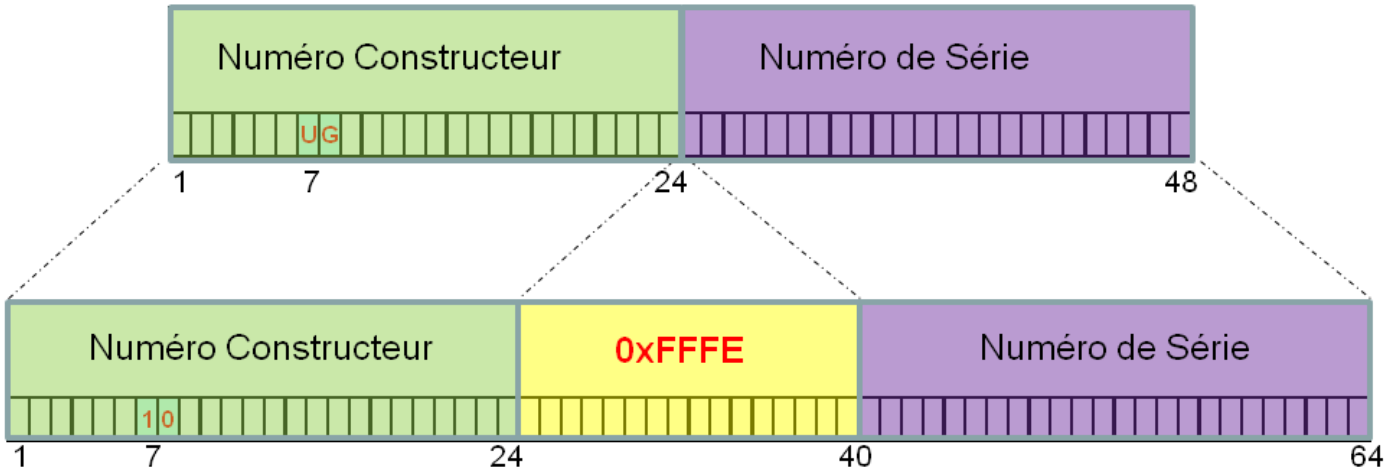
3FFE::**0**F0F:**0000:0000:0000**:**00**A0:1200
ou
3FFE:**0000**:**0**F0F::**00**A0:1200

Simplification 2 :

3FFE::F0F:**0:0:0**:A0:1200
ou
3FFE:**0**:F0F::A0:1200

Identifiant EUI-64 Modifié

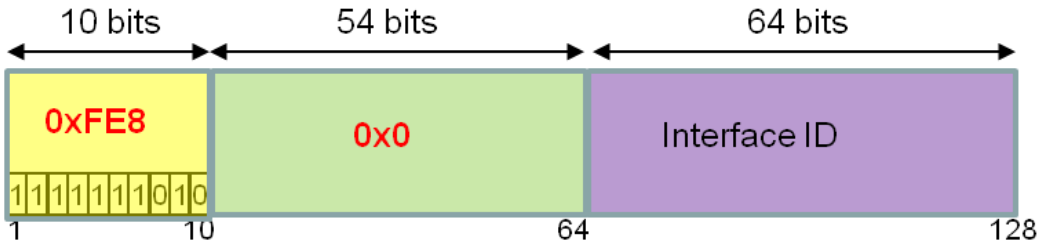
- Un identifiant EUI-64 modifié est formé depuis cette adresse MAC par inversion du bit **u** (*universal/local bit*) et insertion de la valeur hexadécimale sur deux octets **FFFE** entre le numéro constructeur et le numéro d'interface



Identifiant EUI-64 Modifié depuis MAC-48

Adresses Lien-Local

- Au niveau d'un lien, les adresses IPv6 sont formées par concaténation du préfixe ***FE80::/64*** à l'identifiant d'interface au format EUI-64 modifié.



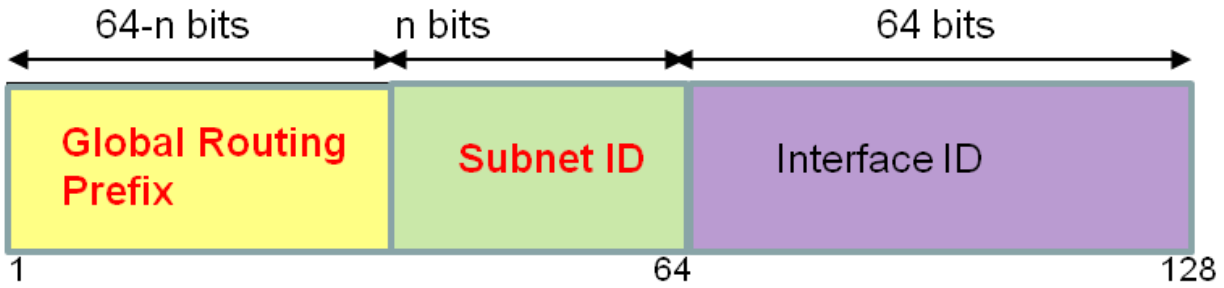
Formation d'une adresse Lien-locale

- L'unicité au niveau lien de l'identifiant d'interface assure ainsi l'unicité de l'adresse IPv6 Lien-local.

- Ce type d'adresse ne traverse jamais les routeurs.

Adressage Unicast : Adresses Globales

- Les adresses Globales sont formées de manière similaire aux adresses Lien-local par ***concaténation du préfixe réseau à l'identifiant d'interface au format EUI-64 Modifié.***



  - **Global routing prefix**: Structuré hiérarchiquement par les RIRs et ISPs. (001/3)
  - **Subnet ID**: structuré hiérarchiquement par les Administrateurs du site.
  - **Interface ID**: identifiant d'interface

Question / Adressage Unicast

- *Adresse MAC : 00-40-96-A7-C5-D3*
- Quel est l'identifiant d'interface ?
- Quelle est l'adresse Lien Local ?
- Son préfixe routable étant 2001:200:0:5004/64 quelle est son adresse globale ?
- Un second préfixe étant 2001:200/32 quelle est l'adresse globale associée ?

Réponse / Adressage Unicast

- *Adresse MAC : 00-40-96-A7-C5-D3*

- Quel est l'identifiant d'interface ?

  *02-40-96-**FF-FE**-A7-C5-D3*

- Quelle est l'adresse Lien Local ?

  FE80::240:96FF:FEA7:C5D3

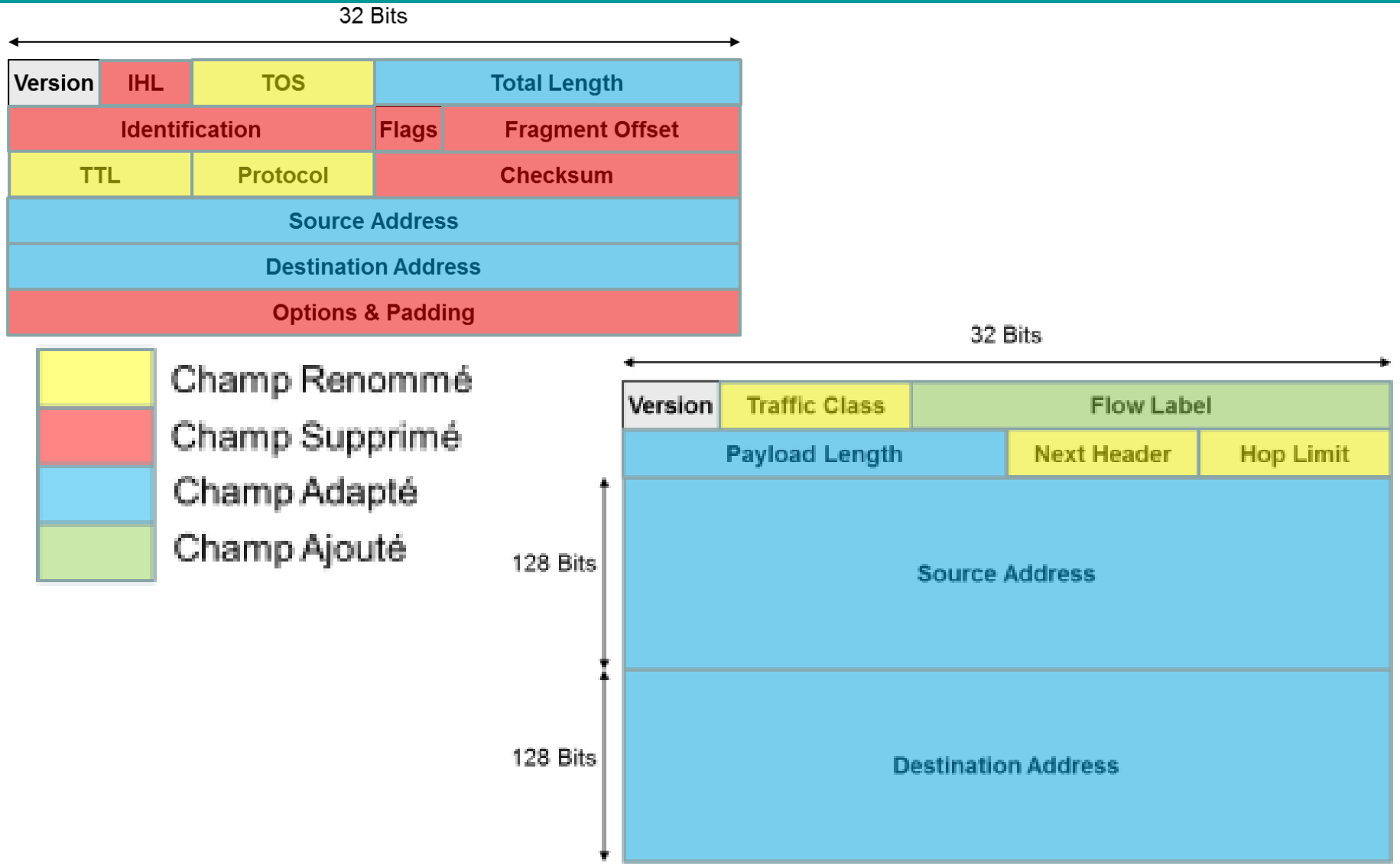
- Son préfixe routable étant 2001:200:0:5004/64 quelle est son adresse globale ?

  2001:200:0:5004:240:96FF:FEA7:C5D3

- Un second préfixe étant 2001:200/32 quelle est l'adresse globale associée ?

  2001:200::240:96FF:FEA7:C5D3

Entêtes IPv4/IPv6



Correctifs sur l'entête Principal

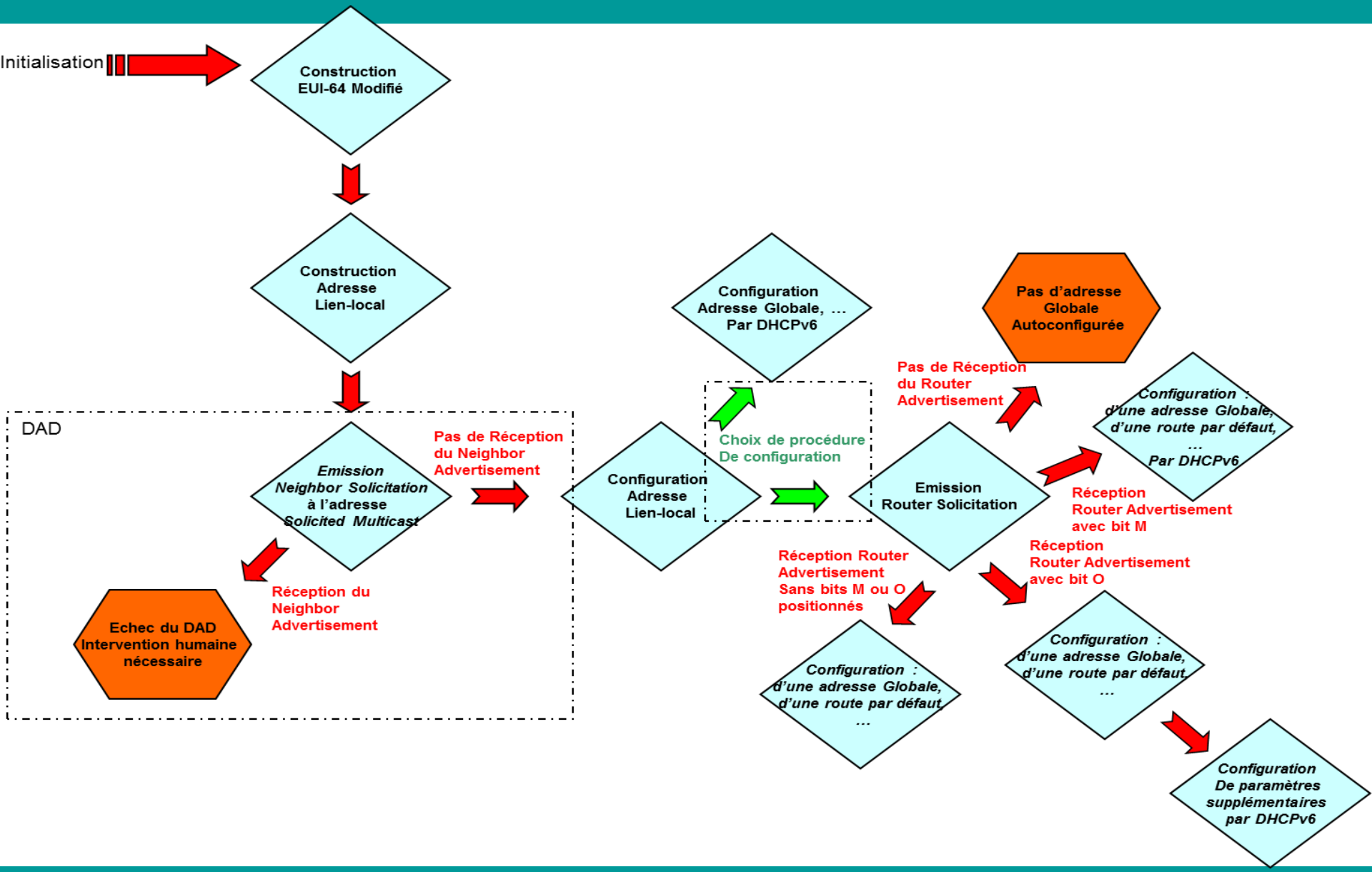
- **Rationalisations**
  - Champ ***Fragmentation*** dégagé de l'entête principale
  - ***Options IP*** dégagées de l'entête principale
  - ***Checksum*** supprimé (recalculé à chaque saut en IPv4 !!)
  - Champ ***IHL*** («***Internet Header Length***») supprimé
  - Champ ***Total Length*** remplacé par ***Payload Length*** qui ne tient plus compte de l'entête principale.
  - ***Alignement modifié*** de 32 à 64 bits
- **Révisions**
  - ***Time to Live*** → ***Hop Limit***
  - ***Protocol*** → ***Next Header***
  - ***Precedence & TOS*** → ***Traffic Class***
  - Adresses 32 bits → 128 bits
- **Extensions**
  - Champ ***Flow Label*** ajouté

=> Passage de 20 octets pour l'entête IPv4 dans sa forme simple à 40 octets pour l'entête IPv6

ICMPv6

- ICMPv6 prend beaucoup d'importance dans IPv6 et permet :
  - la ***résolution d'adresse*** et la ***Détection d'Adresse Double (DAD)*** … intégrés auparavant dans ***ARP*** (***Address Resolution Protocol***) pour IPv4 et à présent au sein du protocole baptisé ***Neighbor Discovery***,
  - la gestion de groupes *multicast* définie auparavant dans ***IGMP*** (*Internet Group Management Protocol*) pour IPv4. Ce mécanisme est à présent nommé ***MLD*** (***Multicast Listener Discovery***),
  - La découverte du ***Path MTU***, par le mécanisme ***Path MTU Discovery***.

DAD & Autoconfiguration sans Etats



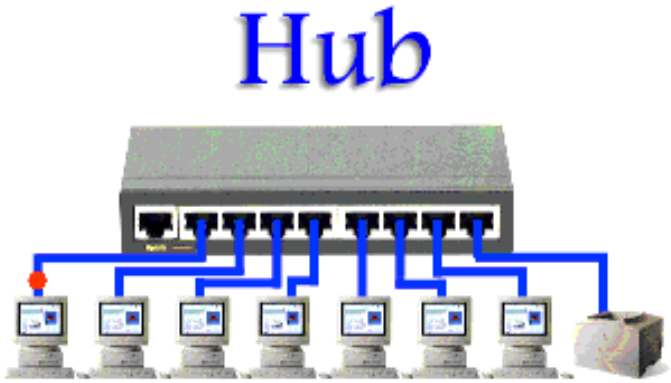
VI - Equipements réseaux

Les éléments d'un réseau

- Les ordinateurs
- Hub
- Switch
- Routeur
- Lien (cable coaxial, fibre optique…)
- Pont réseau (bridge)
- Firewall

Hub

- Equipement au niveau physique (en français: concentrateur)
- Reçoit les trames (paquets de la couche liaison) d'un port et les diffusent (broadcast) sur toutes ses sorties
- Mauvais du point de vue sécurité
- Cet équipement est équivalent au répéteur multiport
- Obsolète



Switch

- Equipement au niveau liaison
- Permet d'offrir plus de la bande passante par rapport au cas où les nœuds partagent le même canal de communication
- Reçoit les trames d'un port et l'envoie juste vers la porte (entrée/sortie) connectant avec la destination correspondante en se basant sur l'adresse MAC
- Utilise la table de contenant les adresses MAC et les sorties correspondantes
- Routage au niveau liaison

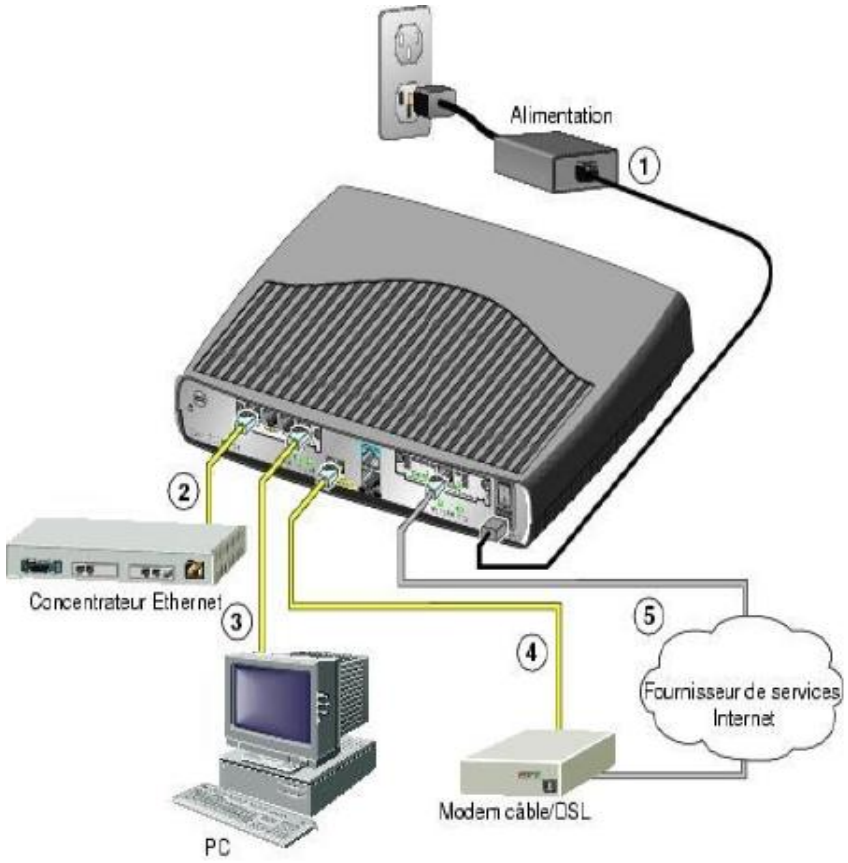
Routeur

Equipement au niveau 3 (IP) destiné au routage

Les paquets circulant entre les réseaux locaux sont dirigés vers leurs destinations par les routeurs

Reçoit les paquets IP et les envoies vers la sortie correspondante

Détermine le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination finale



Hub/switch/Routeur

1

Par **metathesus**, le jeudi 8 janvier 2004 à 19:50:53

3

Salut!

Un hub est un concentrateur et un switch un commutateur...
Quand le hub reçoit une information il l'envoit "partout", alors que le switch qui reçoit une information la redirige uniquement vers le bon destinataire...
Donc un hub a les meme fonctions qu'un switch mais le switch est beaucoup plus performant! Actuellement au vue de la différence de prix entre les deux, il vaut mieux acheter un switch!

Un routeur est comme un switch sauf qu'il y a un port en plus surlequel on branche le modem pour partager une connexion internet aux PC en réseau!

Dans ton cas, achète un routeur qui sera d'un coté relié au modem ethernet et de l'autre à tes PC!
Un routeur permet de "séparer" des réseaux, mais ça c'est une autre histoire plus compliquée qui "ne t'intéresses pas".

Pour les pros... euh... oui c'est très simplifié, c'est pour pas embrouiller...

@pluch! ;-)
There is no problem! Only additional challenges!

Pont réseau (1)

- Equipement au niveau liaison
- Son objectif est d'interconnecter deux segments

de réseaux distincts, soit de technologies différentes, soit de même technologie, mais physiquement séparés à la conception pour diverses raisons (géographique, sécurité, extension de bâtiment ou de site...)

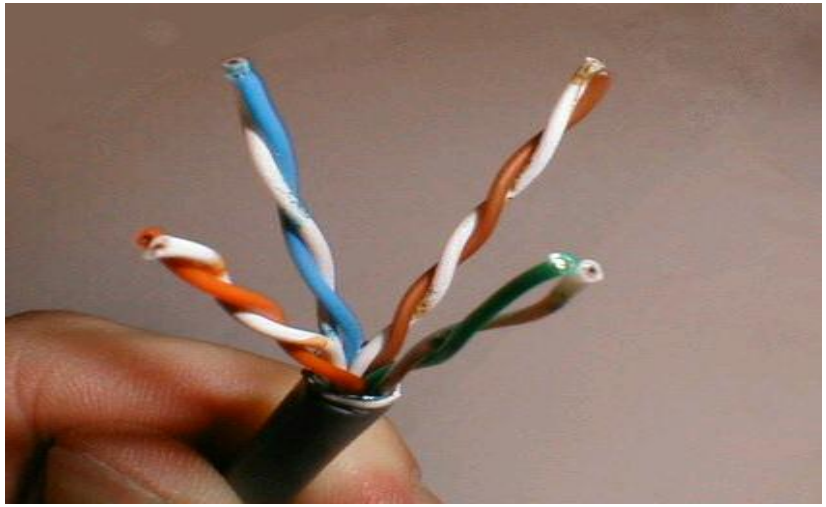
- Il laisse passer les trames d'un réseau à l'autre, mais ne le fait pas bêtement…
- Ses fonctionnalités sont similaires à celles du Switch

Pont réseau (2)

- Un pont, après une période d'apprentissage, sait repérer les adresses MAC des nœuds de chaque côté du pont.

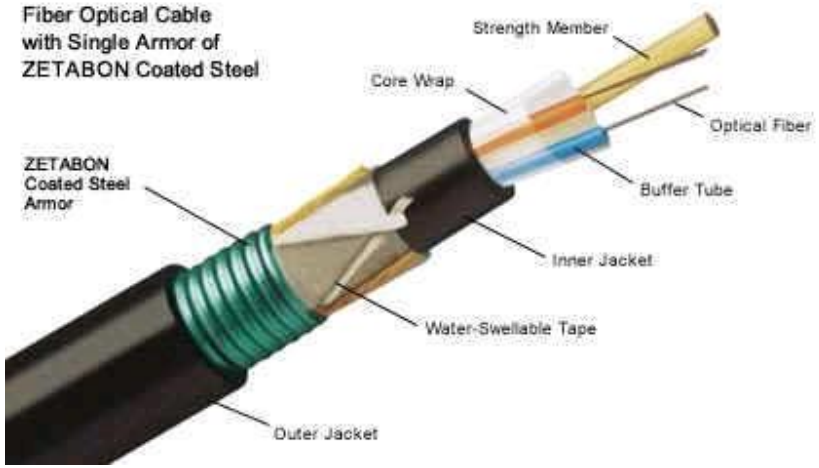
- Il faut **impérativement** que les protocoles réseau soient les mêmes de chaque côté du pont, l'échange se faisant au niveau des trames.
  - Un pont ne pourra pas interconnecter un réseau Ethernet avec un réseau Token Ring par exemple.
  - Un pont ne pourra pas interconnecter deux réseaux Ethernet, l'un utilisant TCP/IP et l'autre un autre protocole (IPX/SPX par exemple).
- Deux réseaux physiques pontés apparaissent **comme un seul réseau physique**. Au niveau de la couche réseau (et des couches supérieures), le pont est transparent. Ceci est un détail fondamental.

Les supports de transmission



Paire torsadée

Cable coaxial



Cable optique

Ondes hertziennes

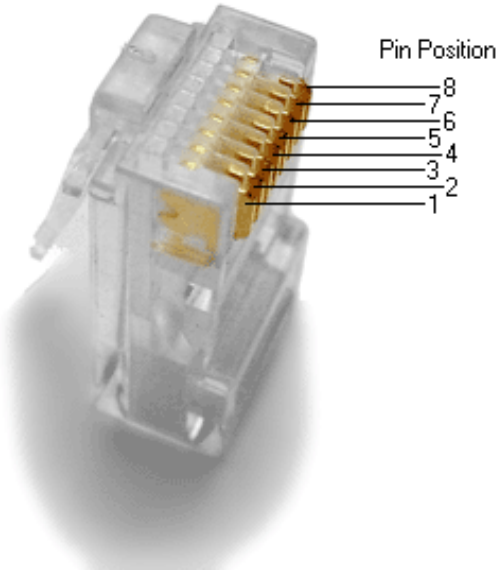
Comparaison des supports de transmission

	Paire Torsadéé	Câble coaxial (bande de base)	Câble coaxial (large bande)	Fibre Optique
Topologie	Anneau,étoile, Bus	Anneau, Bus	Bus, Arbre	Anneau, Etoile, Arbre
Vitesse de transmission	16 Mb/s à 1 Gb/s	16 Mb/s	400 Mhz	500 Mhz à 100 Ghz
Avantage	s'adapte facilement à l'éxistant coût de maintenance faible, coût faible	Grande immunité face au bruit, facile à installer, faible coût de maintenance	Supporte la transmission image, voix , données. Grande immunité au bruit. Physiquement résistant.	Supporte la transmission de l'image, voix et données. Très large bande passante. Grande immunité face au bruit. Très sécurisé.
Désavantage	Peu résistant physiquement. vitesse et distance limitée, faible immunité au bruit et au crosstalk	Peu résistant physiquement. vitesse et distance limitée, plus couteux que la paire torsadée	Très difficile à installer, coût de maintenance très élevé, cout globalement plus élevé que les deux précedents	Très difficile à installer Coût élevé

Connecteur RJ45

Un connecteur **RJ45** est une *interface physique* souvent utilisée pour terminer les câbles de type paire torsadée. « RJ » vient de l'anglais *Registered Jack* (prise jack enregistrée)
Il comporte 8 broches de connexions électriques.

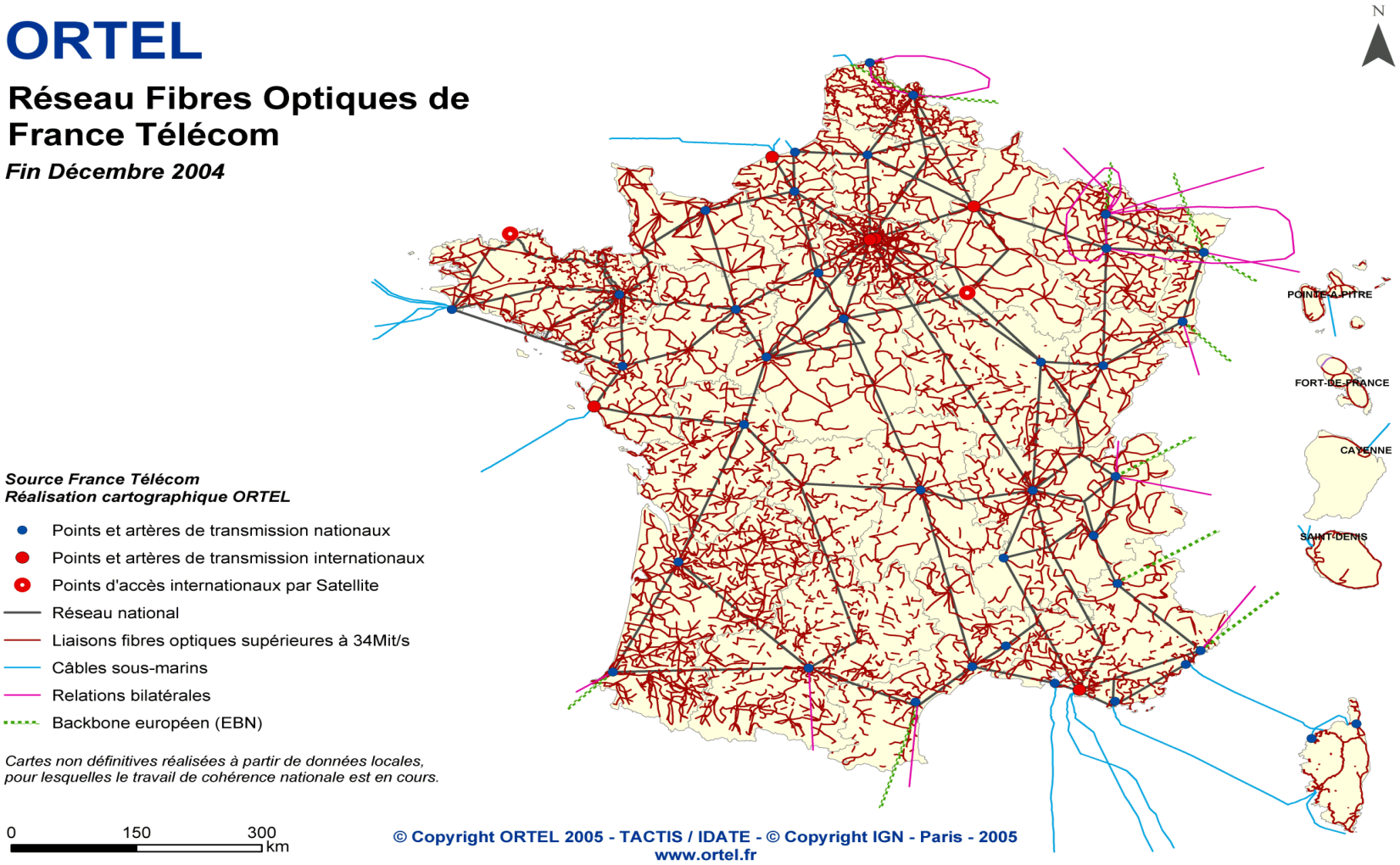
Une utilisation très courante est le câblage Ethernet qui utilise habituellement 4 broches (2 paires). D'autres applications sont par exemple les connecteurs des téléphones de bureaux ou les application de réseaux informatiques comme l'ISDN.



Vitesses de transfert de quelques liaisons

- Liaison parallèle (ordinateur / imprimante) : de l'ordre de 115 Kbit/s
- Liaison série sur un PC : de 75 bit/s à 921 Kbit/s
- Connexion Internet par modem RTC de 14,4 à 56 Kbit/s
- Connexion internet par ADSL : jusqu'à 2 Mo/s en down et 130 ko/s en up
- Liaison wifi sans fil : de 11 Mbit/s à 128 Mbit/s …
- Serial ATA : 150 Mo/s, Serial ATA2 : 300 Mo/s et 600Mo/s
- USB 1.1 : max 12 Mbit/s ; USB 2.0 : max 480 Mbit/s
- Firewire (IEEE 1394) : 400 Mbit/s à 1.5 Gbit/s
- Réseau local : 10 Mbit/s à 100 Mbit/s
- Epines dorsales de réseaux (backbone) :de 500 Mbit/s à 10 Gbit/s
- Réseaux spécialisés : jusqu'à 800 Mbits/s

Réseau de la fibre optique



Résumé des équipements

Couche 3	Routeur
Couche 2	Pont, commutateur (switch)
Couche 1	Répéteur, concentrateur (Hub)