M2102 - Architecture des réseaux (Computer Networks)

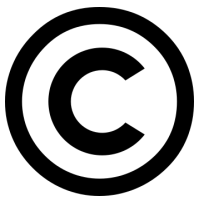
réseaux 1 : Interconnexion des machines et des réseaux

Nicolas Hernandez

Cours de DUT informatique – 1ère année
IUT de Nantes – Département Informatique

Nantes, le June 8, 2020

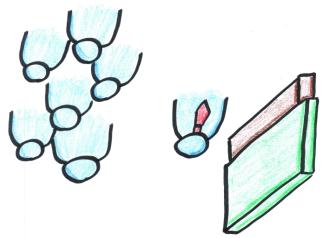
Sommaire

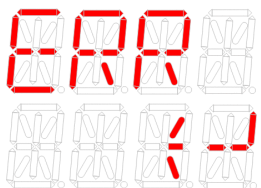


Droit d'auteur sur les ressources pédagogiques[a] : autorisation d'utilisation personnelle

[a] avec des medias issus de `http://commons.wikimedia.org`

Supports fournis en avance, permanence de l'enseignant... privilégier la classe inversée





Le cours et son support évoluent chaque année. Si vous repérez une erreur n'hésitez pas à me la signaler par email : `nicolas.hernandez @ univ-nantes.fr`

Merci de penser à éteindre vos téléphones portables pendant les cours ;-)

Organisation du module

Volume horaire

- 6 semaines, 4x1H20 en promo (CM), 6*1H20 en groupe de TD, 6*1H20 en demi-groupe de TD (TP)

Modalité d'évaluation

- 1 note résultante de la composition de tests/devoirs quasi-hebdomadaires

Equipe pédagogique

- N. Hernandez (resp.), J.-F. Remm, J.-F. Berdjugin, E. Helleu

Support

- `http://madoc.univ-nantes.fr/`

Sommaire : Principes majeurs des réseaux

Objectif du cours

Problème

(Notre objectif sera de) **comprendre comment l'information est acheminée dans un réseau** *informatique d'un expéditeur à un destinataire*

Que se passe-t-il quand je clique sur

- un lien d'une page web depuis mon client navigateur ? Comment ma requête trouve-t-elle la machine qui héberge le serveur que je sollicite dans le réseau local ou sur l'Internet ? Comment l'application serveur est-elle identifiée sur la machine ?
- le bouton "envoyer" de mon mailer ? Comment mon mail est-il acheminé jusqu'au destinataire ?

Un réseau c'est quoi ?

Un **réseau** est un ensemble de machines (e.g. ordinateur, imprimante, frigo) que l'on a **interconnectées** pour leur permettre de **communiquer** entre elles.

L'**interconnexion** entre deux machines est rendue possible via des **liaisons** de diverses natures physiques (e.g. filaire électrique, onde électromagnétique du wifi, fibre optique). Elle est étendue à plusieurs machines via des **équipements multi-ports** (e.g. commutateur, routeur).

Le **problème de l'acheminement** varie selon l'infrastructure physique qui (inter)connecte les machines, la distance entre les machines, les protocoles de communication qu'elles utilisent, les partionnements souhaités pour organiser les réseaux.

Eléments de solution au problème de l'interconnexion 1/4

Emettre un message n'est pas suffisant pour communiquer

- Comment puis-je identifier mon interlocuteur quand je ne le connais pas ? Comment s'assurer que celui-ci est disponible pour m'écouter ? M'a-t-il entendu ? Faut-il que je répète une partie de mon message ? Parle-t-il ma langue d'abord ?
- *Si la communication entre les philosophes transite par plusieurs canaux dont du morse et des signaux de fumée, est-ce que ces philosophes sont censés connaître ces langages ? Si un signal de fumée se dissipe trop vite, est-ce à eux de le "regénérer" ?*

$\hookrightarrow$ Organisation de l'architecture des machines et des équipements en **couches fonctionnelles** (applicative, acheminement distant/inter-réseaux, acheminement local)

Eléments de solution au problème de l'interconnexion 2/4

Différentes situations de communication

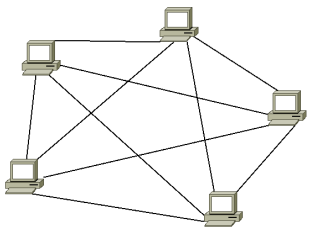
- Différentes infrastructures pour porter la communication (l'air, le morse, les signaux de fumée...), parfois en cascades, des interlocuteurs +- distants
- *Ce n'est pas la même chose de faire discuter un enseignant avec un étudiant dans une salle de classe*[1] *(avec un bruit de fond de bavardage), et deux philosophes, l'un suédois et l'autre philippin, chacun résidant dans leur pays natal.*

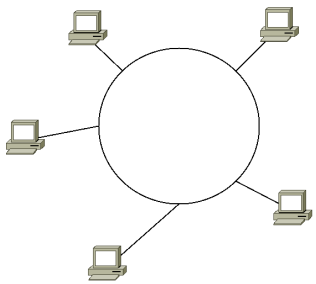
↪ **Des modes d'acheminements distincts** en local et inter-réseaux

[1] Variante : un médecin avec un patient dans sa salle d'attente.

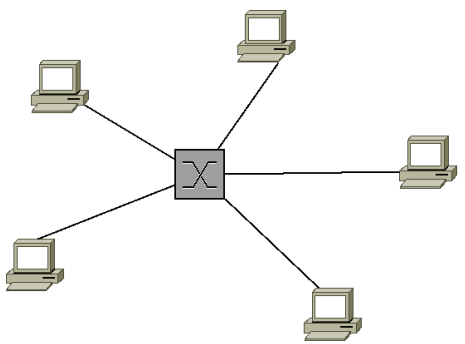
Eléments de solution au problème de l'interconnexion 3/4

- **Accroissement du nombre de connectés**
  - Impossibilité d'établir une liaison physique entre chaque machine
    pour N machine, il faudrait $N(N-1)/2$ liens
  - Difficulté d'interconnecter sur un même canal
    Conflit d'accès au médium (problème de collisions qui conduit à une retransmission)





↪ **Utilisation d'équipements d'interconnexion** qui permettent de réduire le nombre de domaines de collision et partitionner logiquement les réseaux locaux et Internet



Eléments de solution au problème de l'interconnexion 4/4

Accroissement du trafic dans les réseaux à diffusion (i.e. où chacun peut joindre tout le monde)
notamment des messages de diffusion pour la gestion du réseau (découverte du voisinage, annonce de service, mise à jour des caches...)
↪ **Augmentation du débit** dans les réseaux, notamment en travaillant la capacité physique des supports

Sommaire : Principes majeurs des réseaux

Deux clés pour comprendre les réseaux

Pour **comprendre les réseaux/résoudre un incident**(“Je clique mais ça marche pas”), il faut analyser le réseau selon **deux dimensions d’organisation** :

1. **en couches (vue de côté)**
2. **topologique (vue du dessus)**

Organisation des réseaux en couches (vue de côté)

Clé de compréhension

L'**analyse du fonctionnement d'une machine ou d'un équipement réseau requiert de l'appréhender dans sa verticalité**.

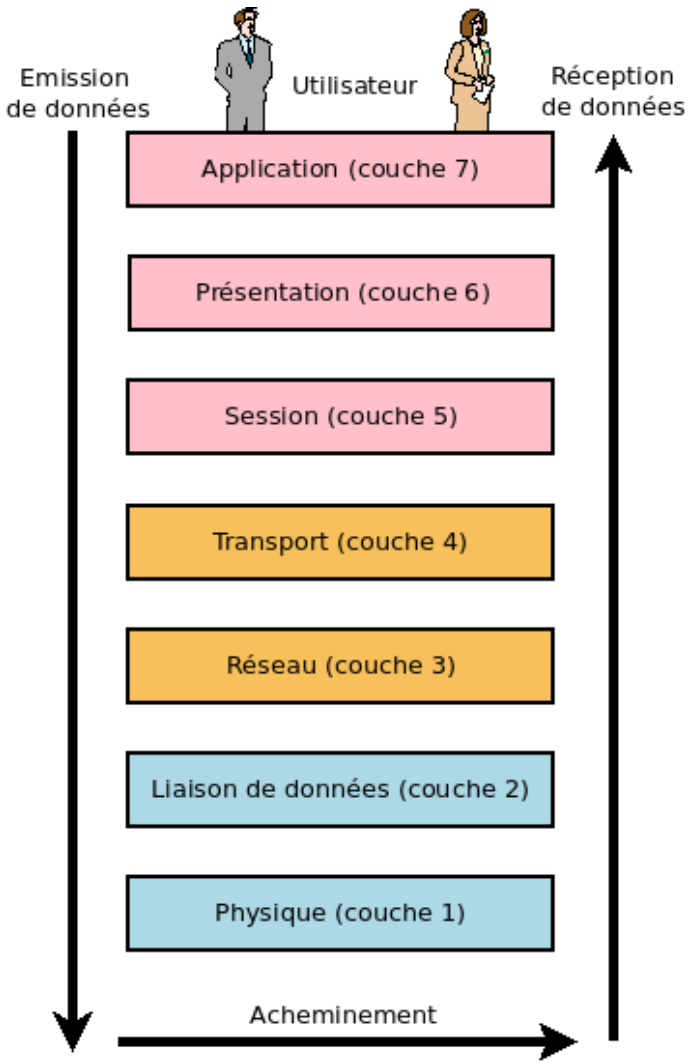
Au moins trois modèles peuvent nous aider :

1. Modèle théorique de référence **OSI de l'ISO**
2. Interconnexion des réseaux **Pile TCP/IP** (couches médianes)
3. Infrastructure des réseaux **IEEE 802** (couches basses)

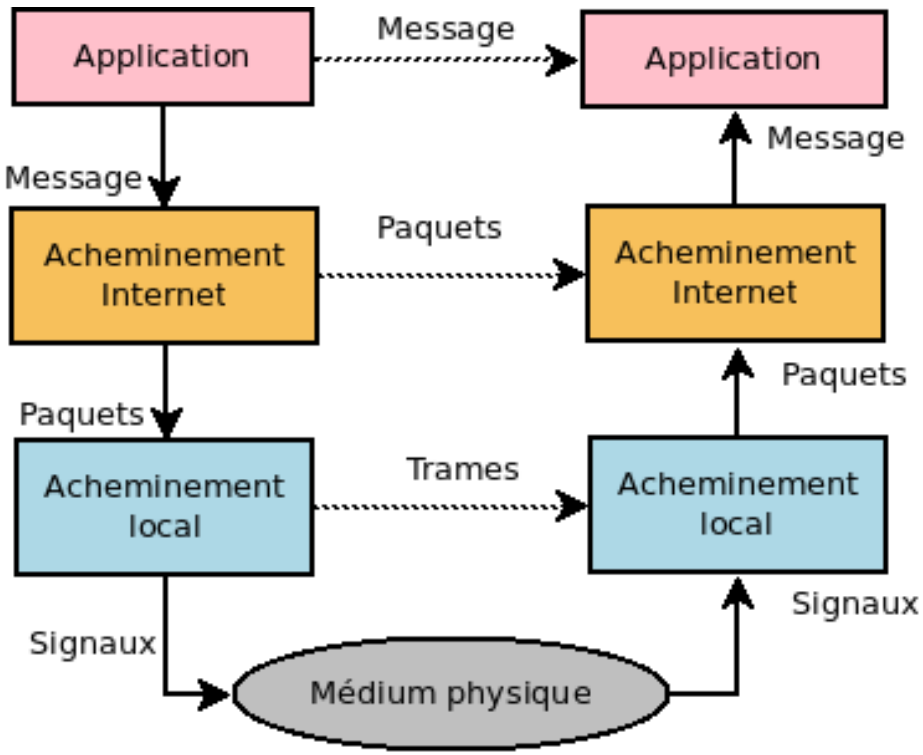
OSI, un modèle de référence... 1/3

Le médium physique ne compte qu'une couche fonctionnelle mais **les machines et les équipements en compte généralement plusieurs**.
On parle d' **architecture en couches ou de pile**

L'*International Standardization Organization* (ISO) propose dans sa norme *ISO 7498* un modèle théorique de référence pour l'interconnexion des systèmes ouverts appelé **Open System Interconnexion (OSI)**



OSI, un modèle de référence, ici simplifié 2/3



Des **couches fonctionnellement distinctes**

Des entités de **même niveau qui parlent le même protocole (langage)** avec une entité homologue distante

mais qui **exploitent les services des couches inférieures** pour communiquer effectivement

OSI, un modèle de référence, ici simplifié 3/3

Applications (niveau 5, 6 et 7 OSI)

- **au service d'un humain ou démon d'un système d'exploitation**
- **distribuées** : un client sollicite un serveur (distant)
- interprètent les paquets rassemblés sous forme de **message**

Acheminement entre les réseaux (niveau OSI 3 Réseau et 4 Transport)

- Offre (en option) une **qualité de service de bout en bout du transport** des messages
- **Identifie un destinataire, et trouver la route pour acheminer les paquets** (fragments d'un message) entre deux machines appartenant ou non au même réseau logique

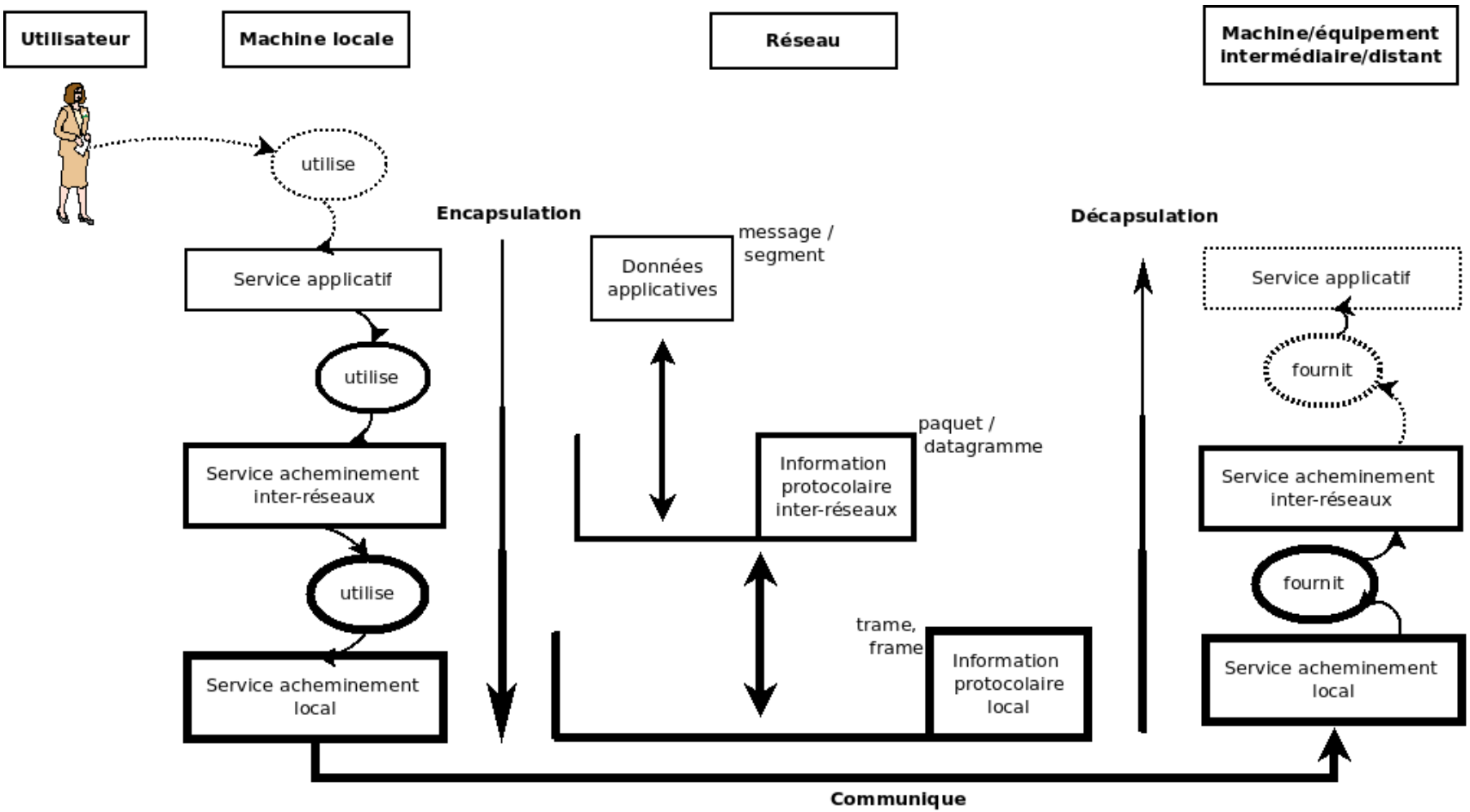
Acheminement dans un réseau (OSI 1 Physique et 2 Liaison)

- **Délivre des trames** (qui portent des paquets) entre deux machines d'un même réseau physique
- **Règle les problèmes posés par l'échange de signaux physiques**

Acheminement vu de côté

Deux opérations entre les couches des architectures des machines et des équipements d'interconnexion : **encapsulation** (en émettant) et **décapsulation** (en réceptionnant)

- Une couche ajoute aux données transmises l'information **protocolaire** nécessaire à sa couche homologue pour que celles-ci puissent assurer leur fonction ou **service**
- Exemples de fonctions : vérification de l'intégrité, acheminement sur réseau local, acheminement sur l'Internet, réassemblage / fragmentation/réordonnancement / récupération si perte, passage à la bonne entité de la couche supérieure...
- Attention : une couche peut avoir plusieurs fonctions (i.e. rendre plusieurs services) et plusieurs instances d'une même fonction (on parle d'**entités**) e.g. le mailer et le navigateur web au niveau application

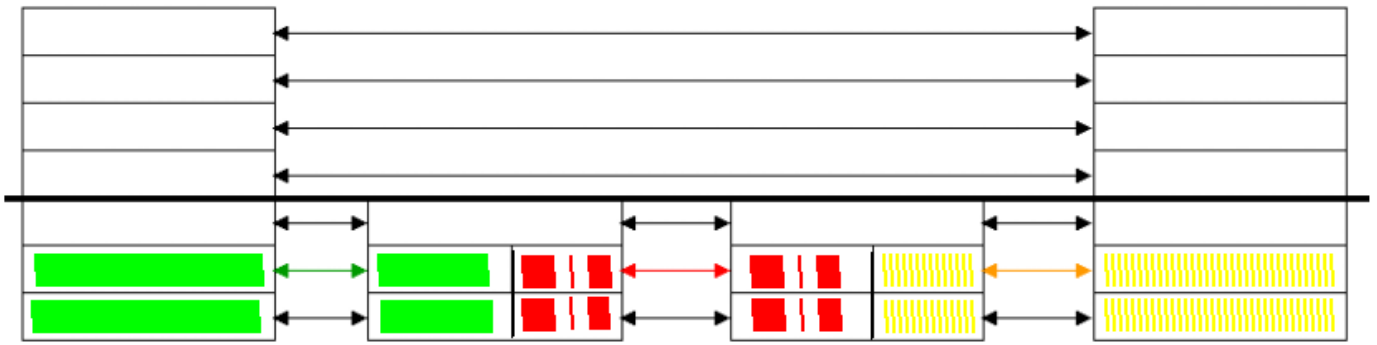

Utilisateur
Machine locale
Réseau
Machine/équipement intermédiaire/distant
utilise
Service applicatif
utilise
Service acheminement inter-réseaux
utilise
Service acheminement local
Encapsulation
Données applicatives
message / segment
Information protocolaire inter-réseaux
paquet / datagramme
Information protocolaire local
trame, frame
Décapsulation
Service applicatif
fournit
Service acheminement inter-réseaux
fournit
Service acheminement local
Communique

Adressage local, Internet et applicatif

Comment identifier un destinataire dans un réseau local ? Sur l'interconnexion des réseaux ? Sur une machine distante ?

Interconnexion	**Couche OSI**	**Information protocolaire encapsulée**
D'applications distantes	4 (Transport)	Numéro de **port** source et destination
De réseaux locaux (Inter-net)	3 (Réseau)	Adresses **IP** source et destination
Au sein du réseau local	2 (Liaison)	Adresses **MAC** source et destination

Acheminement entre des couches homologues hétérogènes



- Possibilité de mises en oeuvre sur des équipements d'interconnexion (routeurs, commutateurs, etc.) de marques différentes et des protocoles hétérogènes : les couches supérieures ne les voient pas
- Exemples d'infrastructures : Ethernet, Wifi, ATM, X.25...

Sommaire : Principes majeurs des réseaux

Organisation topologique du réseau (vue du dessus)

Clé de compréhension

L'analyse du fonctionnement d'une machine, d'un équipement réseau et d'un(e interconnexion de) réseau(x) requièrent d'**observer les schémas d'inter-connexions physiques et logiques mis en place entre les machines et les équipements**.

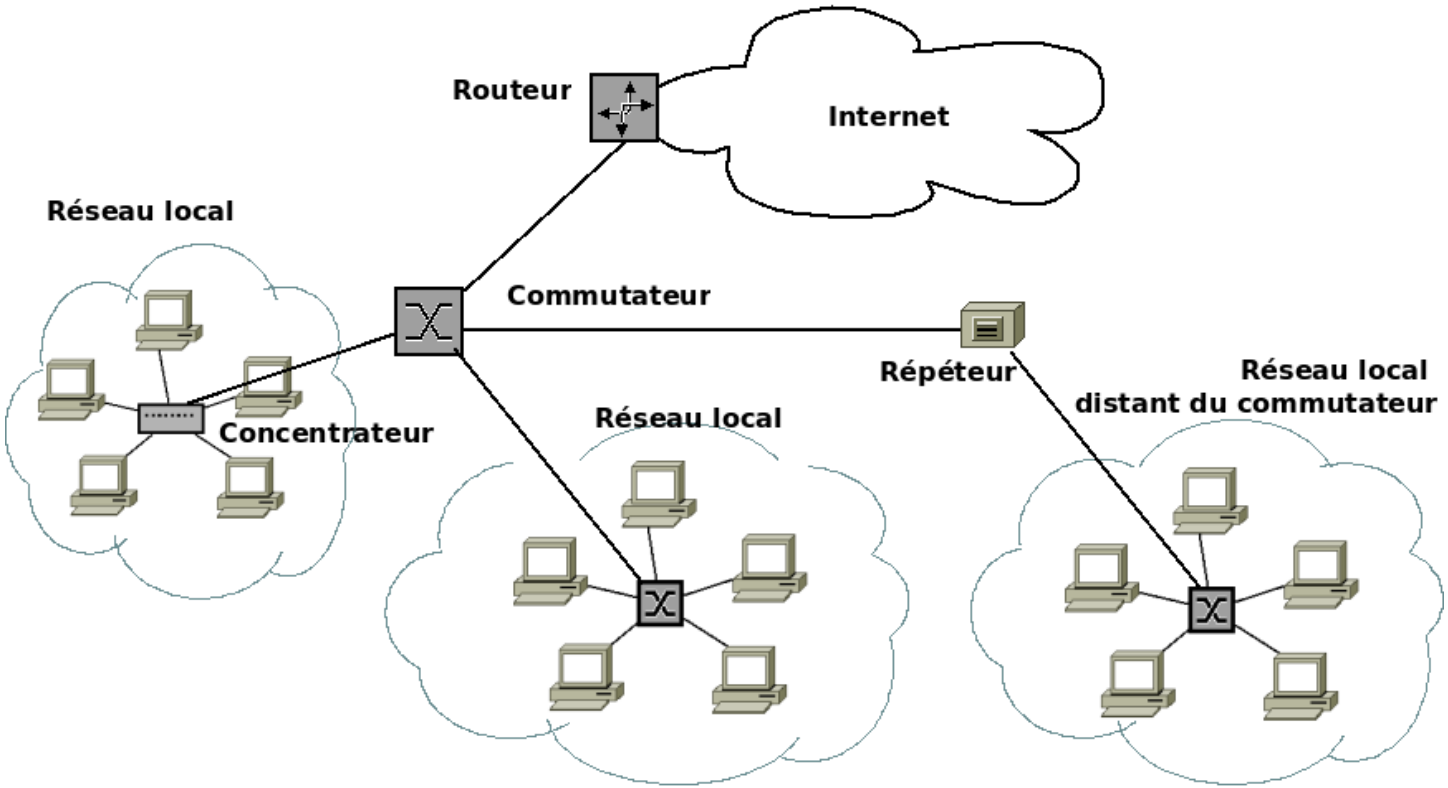
Topologie physique et topologie logique

Le problème d'interconnexion s'aborde à différents niveaux :

- La **topologie physique de la liaison**[2] qui correspond à comment les noeuds (machines et équipements) sont physiquement interconnectés ;
- La **topologie logique au niveau Internet** qui traduit une organisation *fonctionnelle* du réseau physique (i.e. un partionnement en zones d'échange distinctes)

En pratique, c'est le découpage logique souhaité en local ou bien entre plusieurs réseaux locaux qui dirigent le choix des équipements d'interconnexion utilisés au niveau physique

[2] termes synonymes : médium, support, technologie, infrastructure



Ici on a 1 réseau local au niveau de la liaison physique.
Voulons-nous 1, 2, 3 réseaux logiques ou tout autre sous-découpage ?

Domaines de collision et de diffusion

Le niveau physique peut s'analyser plus précisément en :

- **domaine de collision** (on dit aussi de *bande passante*) qui correspond à la zone d'un réseau où les trames envoyées par des machines distinctes risquent de **rentrer en collision** lorsqu'elles accèdent au medium (communiquent)
  En pratique, englobe des composants de niveau 1 OSI et s'arrête aux composants de niveau strictement supérieur (*commutateur, routeur*)
- **domaine de diffusion** qui correspond à la zone d'un réseau où les machines peuvent **communiquer entre elles au niveau liaison**
  I.e. où toutes machines peuvent être contactées en envoyant une trame à l'*adresse de diffusion* de la couche liaison
  En pratique, délimité par des *routeurs* et des *VLAN* (niveau 3 OSI)

Un domaine de diffusion peut englober plusieurs domaines de collision mais pas l'inverse !

Revenons sur la notion de réseau local

Intuitivement on donne souvant la définition suivante de réseau local...

- Un **réseau local** (ou *LAN* - Local Area Network) est un réseau informatique à une échelle géographique relativement restreinte (une salle, un bâtiment, un site d'entreprise, un type de département...)

Pour constituer a minima un réseau local il faut...

- **Interconnecter les machines via des équipements intégrant les niveaux 1** (e.g. cable Ethernet, concentrateur) **à 2 OSI** (e.g. commutateur)
- On retrouve la définition d'un **domaine de diffusion** ; **un LAN est un domaine de diffusion**
- **Internet est une interconnexion de domaines de diffusion...**

Acheminement vu du dessus

On distinguera deux situations

- **au sein d'un réseau local** (niveau 2 OSI liaison)
- et **au sein d'une interconnexion de réseaux** (niveau 3 OSI réseau)

Pour chacune, des procédures pour trouver le destinataire afin d'éviter d'envoyer à toutes les liaisons

Comment trouver un destinataire dans un réseau (local) ?

Solution simple et efficace :

- Au sein des équipements d'interconnexion multiports, **émission sur toutes les sorties** : assure que le destinataire soit atteint mais est loin d'être une solution optimale (accroissement du trafic)

Solution plus complexe mais plus optimale :

- **Transmission via seulement la sortie où l'équipement sait trouver le destinataire** et non à toutes les sorties

Ces solutions régissent l'**acheminement au sein d'un réseau local**.
On parle de **réseau commuté**. Les équipements qui réalisent l'aiguillage ou **la commutation de trames** sont des **commutateurs** (*switch*).

Comment trouver le destinataire au sein d'une inter-connexion de réseaux ?

En dotant les machines et les équipements d'interconnexion des réseaux (les **routeurs**) de moyens pour

- déterminer si un destinataire est joignable sur un réseau local directement accessible
- et sinon **calculer le plus court chemin** pour atteindre un destinataire (via des routeurs voisins) ou s'en rapprocher

C'est ce que l'on appelle le **routage de paquets**

Quizz de synthèse

- A quoi correspond le processus d'encapsulation / décapsulation ?
- à ajouter des en-têtes d'information aux données en provenance de la couche supérieure afin de permettre à la couche homologue de gérer ces données
- A quel niveau OSI est traité l'acheminement des données au sein d'un réseau local ? Au sein d'Internet ?
- respectivement 2 liaison, 3 réseau

Bibliographie

Le présent cours s'appuie sur

Servin ed. 2003 Chapitre 6. Notions de protocoles et 9. Les architectures protocolaires

Pujolle ed. 2005 Chapitre 3. L'architecture générique

Tanenbaum ed. 1996 Sections 1.2. Network Hardware et 1.3. Network Software

Sommaire : Positionnement du cours

A quelles questions répondra ce cours ?

Comment...

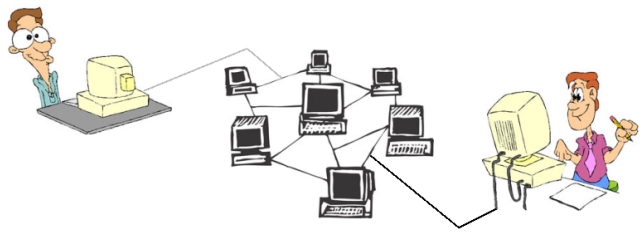
- interconnecter physiquement toutes les machines du monde ?
- permettre à plusieurs machines de communiquer sur une même liaison ?
- identifier une machine sur un réseau local i.e. parmi plusieurs sur une même infrastructure physique ($\Leftrightarrow$ distinguer des personnes qui attendent dans une même salle) ?
- trouver une machine dans un réseau local et lui acheminer une trame d'information ($\Leftrightarrow$ trouver un patient dans une salle d'attente) ?

A quelles questions répondra ce cours (suite) ?

Comment...

- interconnecter des infrastructures différentes, donné le fait qu'il existe plusieurs constructeurs concurrents (IBM, Xerox, ...) ?
- identifier une machine sur le réseau résultant de l'interconnexion de tous les réseaux locaux ?
- trouver une machine dans l'inter-réseaux et lui acheminer une paquet d'information ($\Leftrightarrow$ joindre un homologue résidant dans un autre pays) ?
- s'assurer que les différents paquets d'un même message sont tous bien reçus et ré-assemblés dans le bon ordre ?
- identifier une application réseau sur une machine afin de lui acheminer un message qui lui est destiné (a fortiori si plusieurs instances de l'application tournent en même temps) ?

A quelles questions ne répondra pas ce cours ?



Comment...

- coder l'information à partir d'un signal (la voix est une onde) i.e. transformer de l'analogique en binaire et inversement ?
- découper des flux binaires en trames d'information (unité élémentaire) ?
- détecter et corriger des erreurs de transmission ?
- évaluer la performance d'un canal ?

Positionnement par rapport aux autres UE

Pré-requis en Unités d'Enseignements (UE)

- M1101 - Architecture matérielle - Systèmes d'exploitation - Réseaux Introduction aux systèmes informatiques (JF Hue/Loig Jezequel)

Prolongements

- M3102 - Etude des services réseaux (JF Remm)
- M4101C - Administration système et réseau (N Hernandez)

Positionnement par rapport au PPN 2013*

Contenus

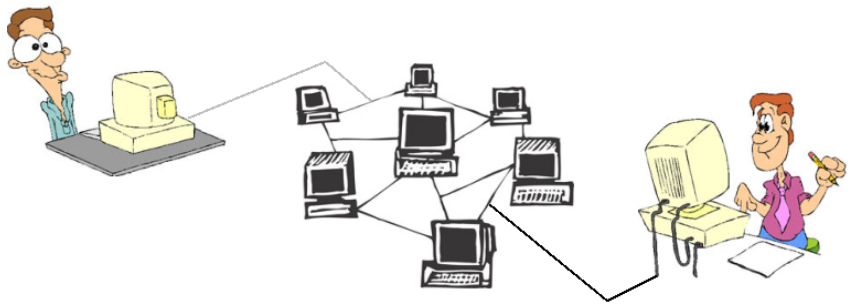
- Architectures des réseaux : modèles OSI et TCP/IP
- Réseaux locaux : Ethernet, WiFi
- Adressage, commutation, routage, transport
- Notions de base en configuration d'un réseau

Modalités de mise en oeuvre

- Observation de communication réseaux in vivo (capture de trames et observation des niveaux d'encapsulation)
- Conception de plans d'adressage avec sous-réseaux
- Diagnostique de problèmes de connexion
- Mise en place d'un réseau avec configuration des machines et des routeurs

*PPN : Programme Pédagogique National

Ce qui est encore présent dans le nouveau PPN



Comment...

- évaluer les performances d'une liaison physique ? *NON*
- vérifier l'intégrité des trames transmises ? et comment corriger celles en erreur ? *NON*
- arbitrer l'accès au medium par plusieurs machines ? *Peut-être...*
- identifier des trames d'information dans un flux binaire ? *NON*
- comment représenter l'information en général ? *OUI*
- coder l'information à partir d'un signal ? *NON*

Haut

Bas

Bibliographie

Ouvrages disponibles à la bibliothèque de l'IUT (entres autres + références données en fin de chaque poly.)

- A. Tanenbaum, Réseaux, Pearson, 2008 (4e Ed.) et 2011 (5e Ed.) (Exo)
- G. Pujolle, Initiation aux réseaux, Eyrolles, 2002, 2011 (7e Ed.) (Exo)
- C. Servin, Réseaux et Télécoms, Dunod, 2003, 2006, 2009 (3e Ed.)
- J. Dordoigne, Les réseaux Entraînez-vous à l'administration d'un réseau, TP, 2008 (2nd Ed.) et 2011 (3e Ed.)(Exo)
- B. Petit, Architecture des réseaux, ellipses, 2010 (3e Ed) (Exo)
- S. Lohier et D. Présent, Transmission et réseaux, 2010 (5e Ed.) (Exo)
- R. Dapoigny, ...

mais aussi quelques revues mensuelles

- LINUX'mag (www.gnulinuxmag.com), MISC (www.miscmag.com), Hakin9 (hakin9.org), ...

Sociétés savantes

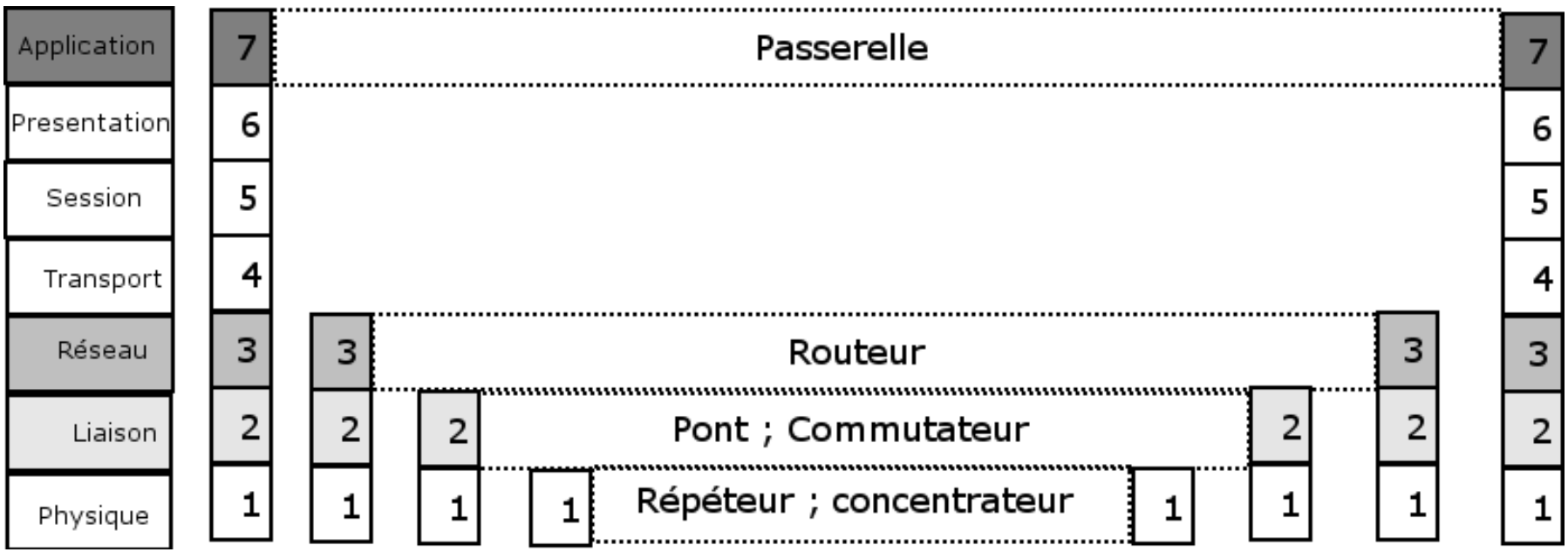
"*pour se comprendre il faut parler une même langue*"

- **International Standardization Organization (ISO)**
  - Regroupe les organismes nationaux tq Association Française de NORmalisation (AFNOR), *American National Standards Institute* (ANSI)
  - Exemples de normes : désignation de filets de pêches (ISO 1530), tailles des sous-vêtements masculins et féminins (ISO 4415 et 4416), modèle théorique de référence pour l'interconnexion des systèmes ouverts (OSI – Open System Interconnexion) (ISO 7498)
- **Institute of Electronic and Electricity Engineers (IEEE "i3e")**
  - Essentiellement des normes sur les réseaux locaux : notamment 802.3 CSMA/CD (Ethernet), 802.5 token ring
- **Request For comments (RFC)**
  - Notes techniques, à l'initiative d'experts (ISO, IEEE, ...), révisés par la communauté Internet
  - `www.rfc-editor.org` (en français `abcdrfc.free.fr`)
  - E.g. IP (RFC791), DNS (RFC1034), HTTP (RFC1945), SMTP (RFC821)

Les questions auxquelles on va essayer de répondre :

- Comment interconnecter plusieurs stations pour former un réseau local ?
- Comment interconnecter des réseaux de protocoles semblables (e.g. Ethernet) avec éventuellement des débits et des supports distincts (câble coaxial, paire torsadée, fibre optique) ?
- Comment étendre un réseau local sur de grandes distances sans diminution du signal ?
- Comment interconnecter des réseaux ayant des architectures de services et de protocoles différentes ?
- Comment réunir plusieurs réseaux locaux en un seul ?
- Comment partitionner un réseau en sous réseaux locaux ?
- Comment interconnecter un réseau local à l'Internet ?

Equipements relais et couches du modèle OSI



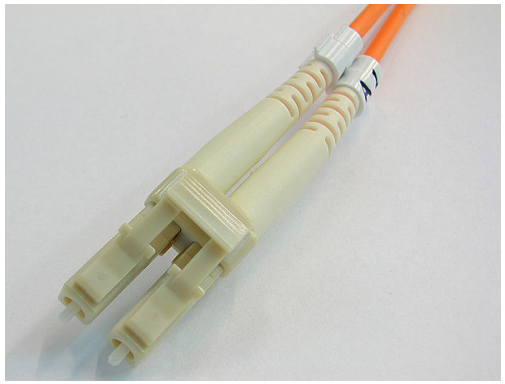
Note : l'ambiguïté des termes vient du fait qu'un même équipement peut cumuler plusieurs fonctions

Sommaire : Equipements relais/d'interconnexion

Câbles Ethernet

← câble coaxial et connecteurs BNC male et femelle

fibre optique avec câbles d'émission et de réception →



← câble Ethernet RJ45

Câbles Ethernet

`DEBIT-Base-TYPE`

- `DEBIT` : en (Méga/Giga) bits per sec (bps) ; 10Mbps (Standard Ether.), 100 (Fast Ether.), >1000 (Ether. Gigabit)
- `TYPE` : coaxial, T (*Twisted*/paires torsadées), F/X (*Fiber*/Fibre optique)

Câbles Ethernet

Câble coaxial

- 10Base2, fin, segment de 200 yards (185 m) et 30 noeuds par segment
- 10Base5, épais, 500 m, 100 n

Paires torsadées

- Catégorie 3 (10 Mbps), cat. 5 (100 Mbps), cat. 5e (1 Gbps), cat. 6a (10 Gbps), 100 m
- vers la cat. 7 (10 à 100 Gbps avec une plus grande bande passante) mais manque de rétro-compatibilité (2018)

Catégories de fibres optiques (diamètre du coeur et longueur d'onde utilisée)

- Multimode, les 1ères sur le marché, coeur de 50 à 62,5 μm pour le bas débit et courte distance, 1Gbps sur 1km
- Monomode, plus complexe (9 μm), moins de réflexion sur la gaine, moins de perte, plus chère, jusqu'à plusieurs dizaines de km

Câbles Ethernet

Nom	**Type**	**Longueur***	**Nb. de noeuds***
10Base5	Coaxial épais	500 m	100
10Base2	Coaxial fin	185 m	30
10Base-T	Paire torsadée	100 m	1024
10Base-F	Fibre optique	2000 m	1024
100Base-T	Paire torsadée	100 m	
1000Base-LX	Multimode fiber	550 m	
1000Base-LX	Single-mode fiber	5 km	
1000Base-ZX	Single-mode fiber at 1,550 nm wavelength	70 km	

* maximale d'un/par segment

En pratique : câbles coaxiaux et 10Base obsolètes, 100Base-TX (réseau local e.g. salle machine étu), 1 Giga (entre serveurs ou avec le backbone), 10 Giga (serveur et son backup, intercontinentale et Joffre/Fleuriaye)

Répéteurs (*repeater*)

convertisseur BNC-RJ45

- Couche : 1, physique
- Fonction :
  - **accroissement de la portée** (e.g. régénération du signal et récupération de l'horloge)
  - et parfois aussi **liaison entre deux câbles de type différent** (e.g. passage coaxial à fibre optique)
  - Interconnexion : locale (extension du domaine de collision et de diffusion) ; aucune incidence sur les protocoles transportées

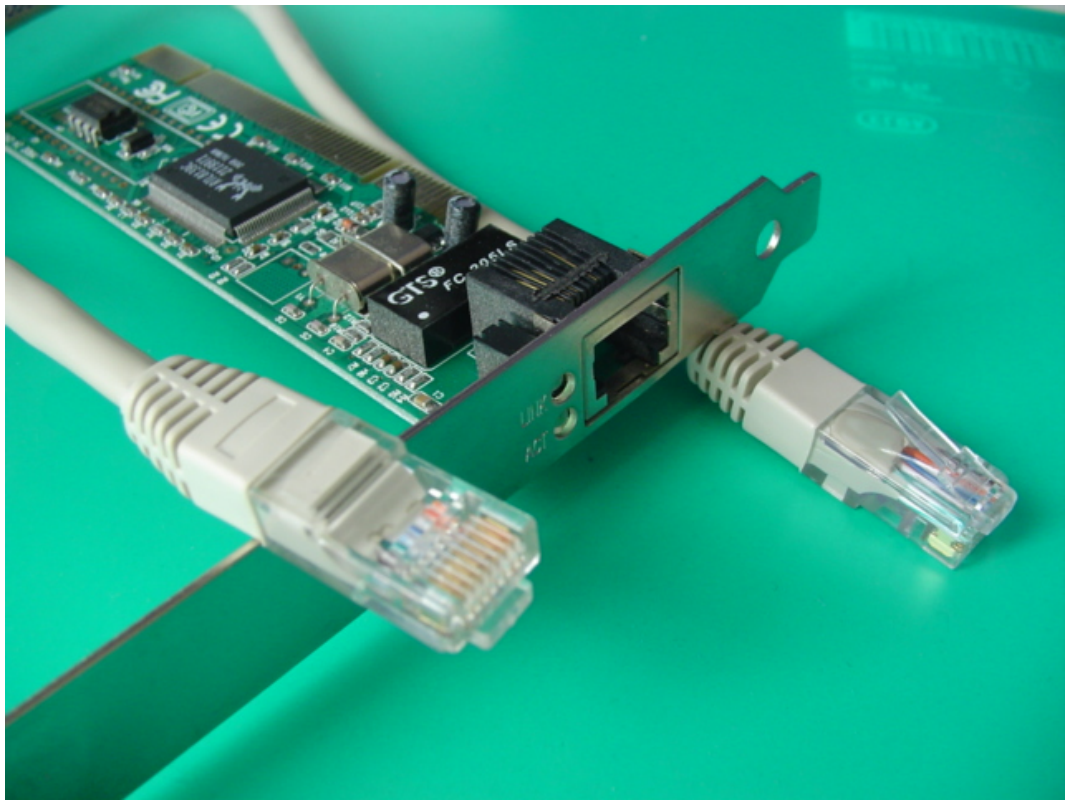
Aujourd'hui, équipement inutile avec Ethernet câblée (on utilise la fibre).
Il existe cependant des répeteurs wifi

Concentrateur (*hub*)

- Couche : 1, physique
- Ports : multiple
- Fonction :
  - **“répéteur” qui transmet toutes les trames sur tous les ports excepté celui d’origine**
  - Interconnexion : locale (même domaine de diffusion et de collision), stations utilisant une topologie en étoile

Sommaire : Equipements relais/d'interconnexion

Cartes réseaux



carte câble Ethernet RJ45

Pont (*bridge*)

- Couche : 2, liaison
- Ports : deux
- Fonction :
  - **"Pontage" : adaptation de débit et de support entre réseaux semblables (e.g. Ethernet paire torsadée /Ethernet fibre optique) ou dissemblables (e.g. Ethernet/Token Ring)**

Aujourd'hui n'est plus un équipement particulier mais avant tout une fonction possible des commutateurs

Commutateur (*switch*)

- Couche : 2 ; Ports : multiple
- Fonction : la **Commutation** i.e. **aiguille sur le port de sortie qui permet d'atteindre le destinataire** (différence avec concentrateur)
- **Au coeur des réseaux locaux**, remplace le concentrateur pour interconnecter les machines,
  - rend caduc l'utilisation de CSMA/CD,
  - rend plus difficile l'espionnage du réseau (*sniffing*)
- Le réseau téléphonique historique s'appelait **RTC** pour **Réseau Téléphonique Commuté** (des circuits électriques raccordés par des opérateurs humains)

Commutateur (*switch*)

Fonctions d'interconnexion :

- **Faculté de non retransmission des trames erronées** (erreurs checksum, trame incomplète suite à une collision)
- **Unification des domaines de diffusion et segmentation en domaines de collision** bien distincts ; i.e. réunit des réseaux locaux éparpillés **en un seul et unique réseau de diffusion**
- **Partitionnement possible des ports en plusieurs domaines de diffusion** aussi appelés **VLAN (Virtual Lan)**
- **Routage** dans certains cas ils sont alors de niveau 3 OSI

Commutateur et acheminement des trames

Comment le commutateur sait sur quel port rediriger une trame ?

- **commutation statique** : table d'acheminement décidée au préalable par un humain
- ou **dynamique** : via *backward learning algorithm* – apprentissage automatique *a posteriori* de la localisation des stations par *examen des trames entrantes* et *association de leur adresse MAC source au port d'entrée* ;
  les trames broadcast (à l'attention de tous) et celles dont le destinataire est inconnu dans la table sont redirigées vers tous les ports excepté le port d'entrée
  (ne renvoie pas si sait le destinataire accessible via le port d'entrée)

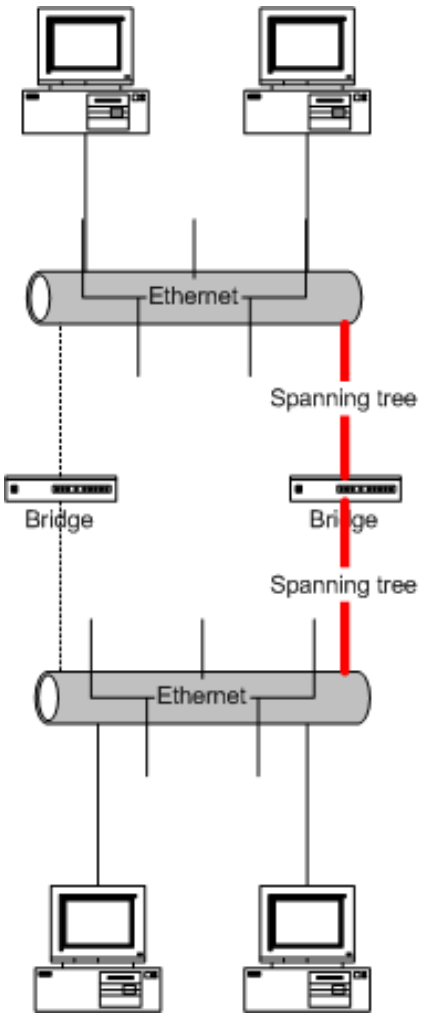
Commutateur et optimisation des ressources

- Possibilité de transmettre **plusieurs trames en même temps si pas via les mêmes ports de sortie**
- **Deux modes de transfert**
  - différé (*store-and-forward*) : stocke l'intégralité de la trame pour l'analyser avant de la ré-expédier (filtre les trames endommagées)
  - direct (*cut-through*) : commence à ré-expédier avant arrivée complète de la trame (traite plus rapidement)
- **Mécanisme Ethernet d'auto-négociation des paramètres optimums de communications** (tel que la vitesse et le mode duplex) entre deux équipements connectés
  le mode de transmission le plus rapide supporté par les deux et le mode full-duplex sont préférés

Commutateur et sûreté

Comment **éliminer les boucles** résultantes du duplexage de matériels (ponts en parallèle) lié à la volonté de rendre plus sûr les systèmes ?

- le **Spanning Tree Protocol (STP)** permet de contrôler les ponts actifs et de basculer le trafic sur les ponts en sommeil en cas de défaillance d'un pont actif
- à partir d'un pont actif élu l'algorithme du Spanning Tree détermine les plus courts chemins en éliminant les boucles (ponts endormis)



VLAN (Virtual LAN (Local Area Network))

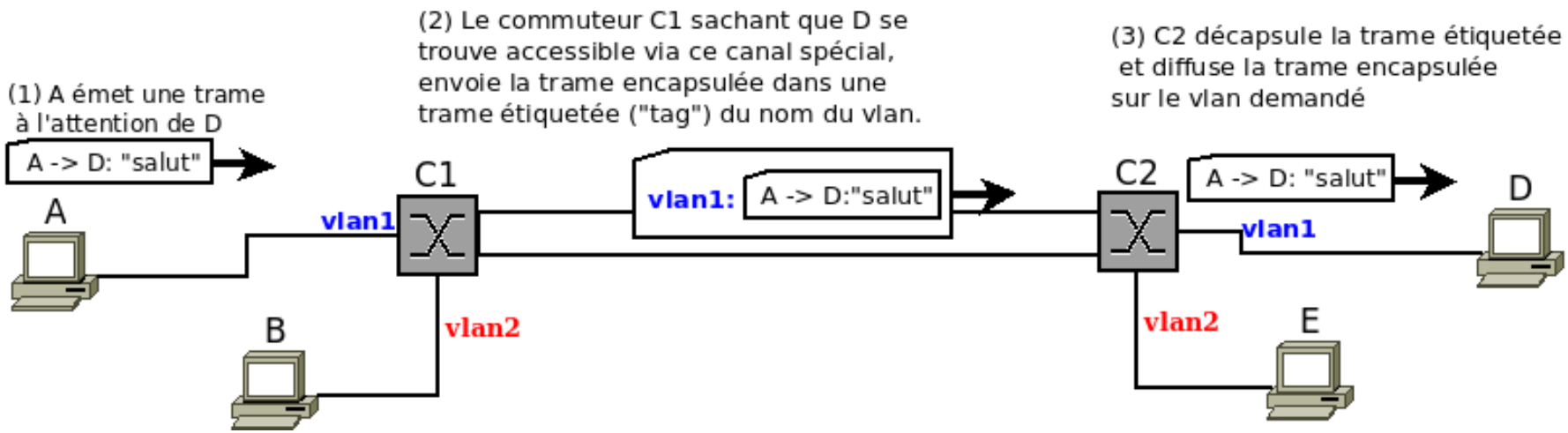
Les VLANs permettent de définir (configuration statique et manuelle) **au sein d'un commutateur quels ports ou quelles adresses MAC ou IP peuvent discuter ensembles**.
En d'autres termes, **un VLAN est la définition d'un domaine de diffusion**.

- Associé à certains **ports** (niveau 1 OSI) : les machines connectées derrières ces ports peuvent communiquer entre elles
- Associé à des **adresses MAC** (niveau 2 OSI) : les machines avec ces adresses peuvent communiquer entre elles
- Idem pour vlan associé à des **adresses IP** (niveau 3 OSI)

Un VLAN permet donc d'organiser logiquement des machines entre elles.
Il existe une version, appelée **VLANs "tagués"** qui permettent d'étendre des domaines de diffusion...

VLANs "tagués"

Les **VLANs "tagués"** ("étiquetés" en français) offrent la possibilité d'**augmenter le nombre des ports** d'un VLAN en mettant en cascade des commutateurs **ou d' interconnecter des VLAN distants**.



Une connexion entre deux ports des commutateurs est réservée.
Les trames y circulent encapsulées dans une trame tierce avec un étiquette indiquant le numéro de VLAN d'appartenance.
Ce **marquage suit la norme IEEE 802.1Q**.

Sommaire : Equipements relais/d'interconnexion

Routeur (*router*)

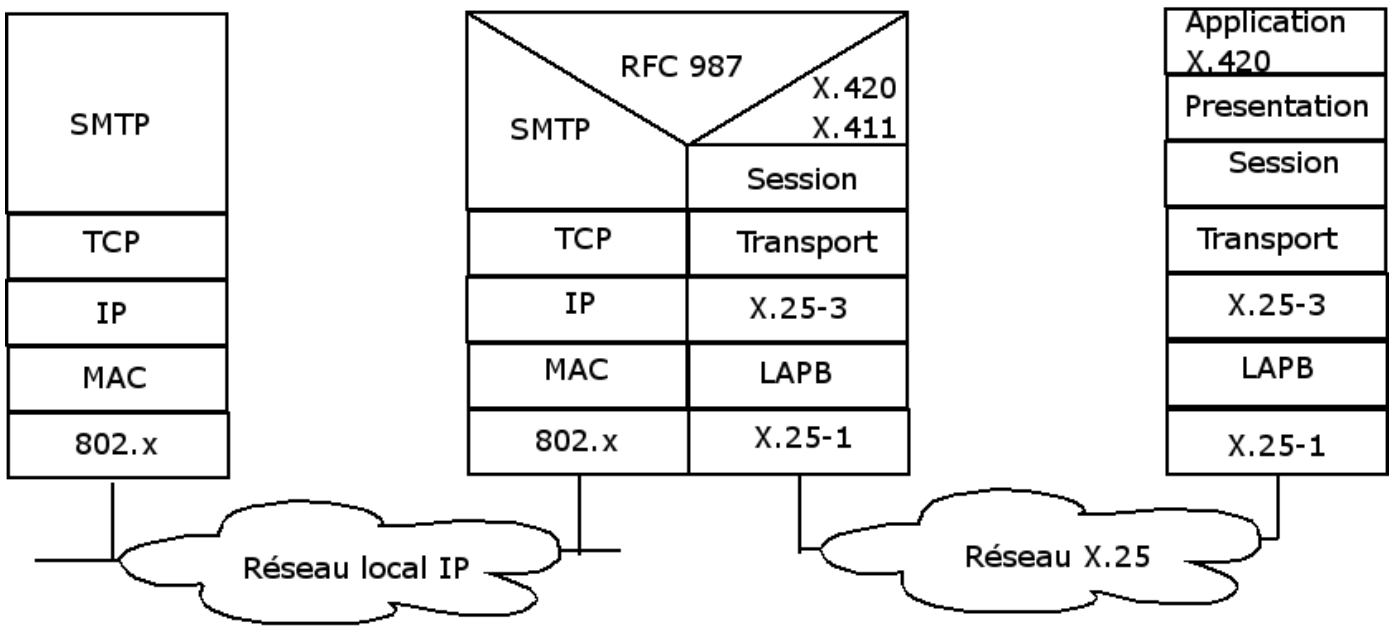
- Couche : 3, réseau/internet
- Fonction :
  - **acheminer les données vers un destinataire** connu par son adresse de niveau 3 (e.g. IP) ;
  - **trouver la (meilleure) route** vers ce destinataire
  - **relayer des paquets entre réseaux d'espace d'adressage homogènes** (e.g. IP/IP) ;
  - **L'interconnexion d'espaces d'adressage non homogènes est non définie au niveau 3 mais pris en charge aux niveaux supérieurs (gateway)** e.g. IP via X.25 (chaque constructeur apporte sa solution ; un routeur peut incorporer cette fonction)
- Point d'accès aux réseaux

Note : la notion d'*espace d'adressage* sera vu dans un autre CM

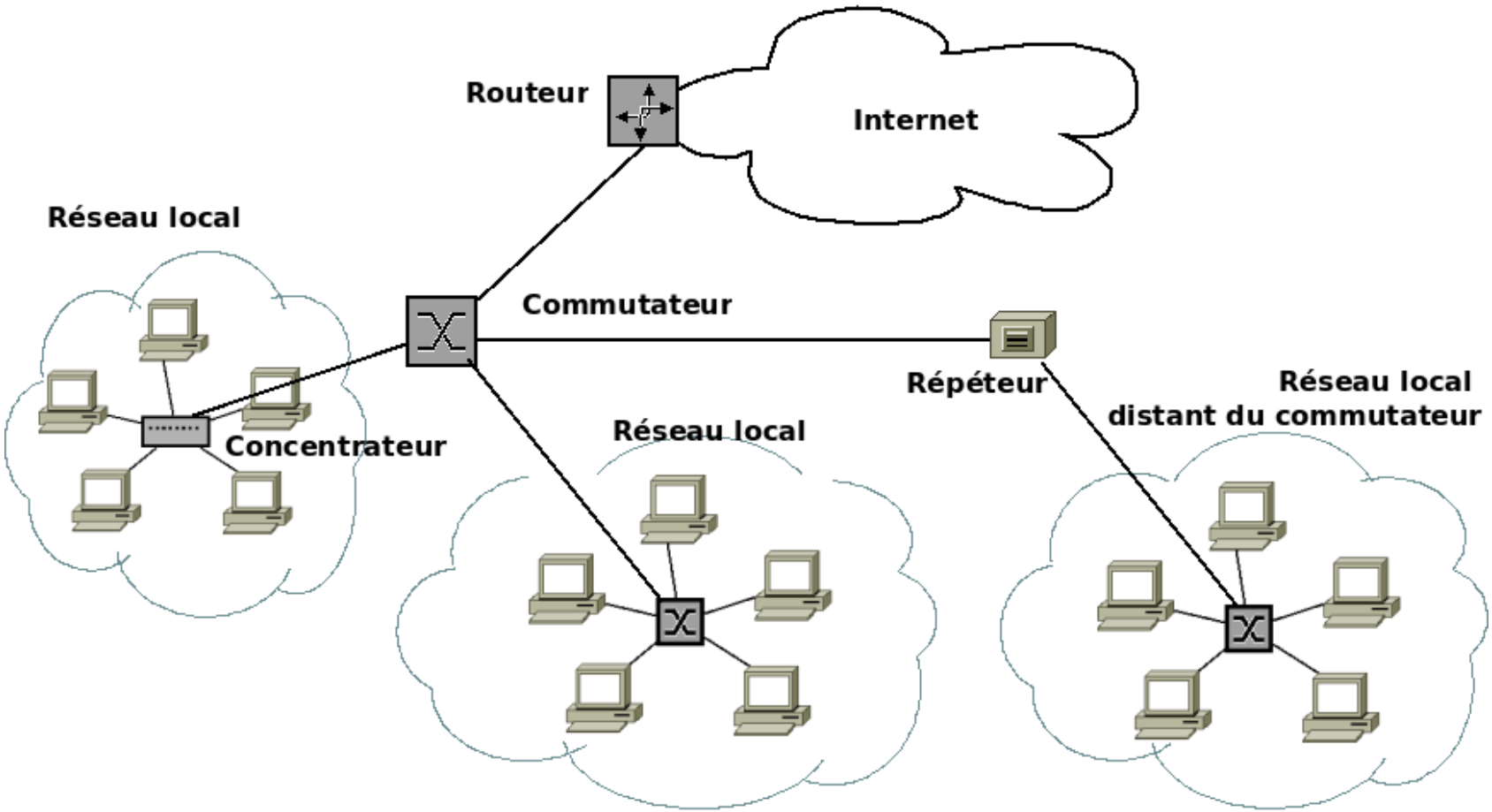
Routeur (*router*)

Passerelle (*gateway*)

- Couche 4 et au dessus (en général applicatif)
- Fonction :
  - **Adaptation des protocoles**
    - E.g. messagerie SMTP (Simple Mail Transfer Protocole) du monde Internet et une messagerie ISO X.400
    - E.g. IP vers X.25



Equipements relais – en résumé



Quizz de synthèse

- Donner quatre noms d'équipement relais intervenant à des couches différentes ? Indiquer un exemple de fonction pour chacun.

Infrastructure des réseaux : le modèle IEEE 802
Différentes propriétés d'un canal de communication
Accès au médium filaire en l'absence de canal full-duplex

Sommaire : Infrastructure des réseaux le modèle IEEE 802

Infrastructure des réseaux : le modèle IEEE 802

Infrastructure des réseaux : le modèle IEEE 802

Les **normes IEEE 802 décrivent le modèle d'infrastructure physique des réseaux locaux que l'on retrouve dans l'Ethernet, le Token Ring, le Wi-Fi, les VLANs.**

- Niveau 2 OSI : **Couche liaison** – IEEE 802.2
  - 2.2 OSI : **Logical Link Control** (LLC)
  - 2.1 OSI : **Medium Access Control** (MAC)
- Niveau 1 OSI : **Couche physique** i.e. le médium – IEEE 802.x

Focus sur la couche Liaison du modèle IEEE 802

Fonctions des **deux sous-couches** de la **couche Liaison** :

- 2.2 OSI : Logical Link Control (LLC)
  - **Identification des trames dans le flux binaire** (encapsulation/désencapsulation des paquets dans/depuis les trames)
  - **Vérification de l'intégrité des trames** (détection et correction des erreurs de transmission ; Hamming, CRC (Codes Cycliques Redondants))
- 2.1 OSI : Medium Access Control (MAC)
  - **Arbitrage de l'accès au médium par plusieurs machines** (CSMA/CD) – IEEE 802.3
  - **Couche optionelle...**

Infrastructure des réseaux : le modèle IEEE 802

Focus sur la couche Physique du modèle IEEE 802

Fonction de la couche **Physique** (1 OSI)

- Dépend des **propriétés d'une liaison physique** (nature : série ou parallèle ; exploitation : simplex, half/full-duplex ; transmission : synchrone ou asynchrone)
- **Codage de l'information et traitement du signal** (encodage analogique ou numérique, représentation des signaux périodiques, bande passante et largeur de bande, modulation et valence)
- **Evaluation des performances d'une liaison physique** (débit, latence, taux d'erreurs)

simplex, half-duplex et full-duplex

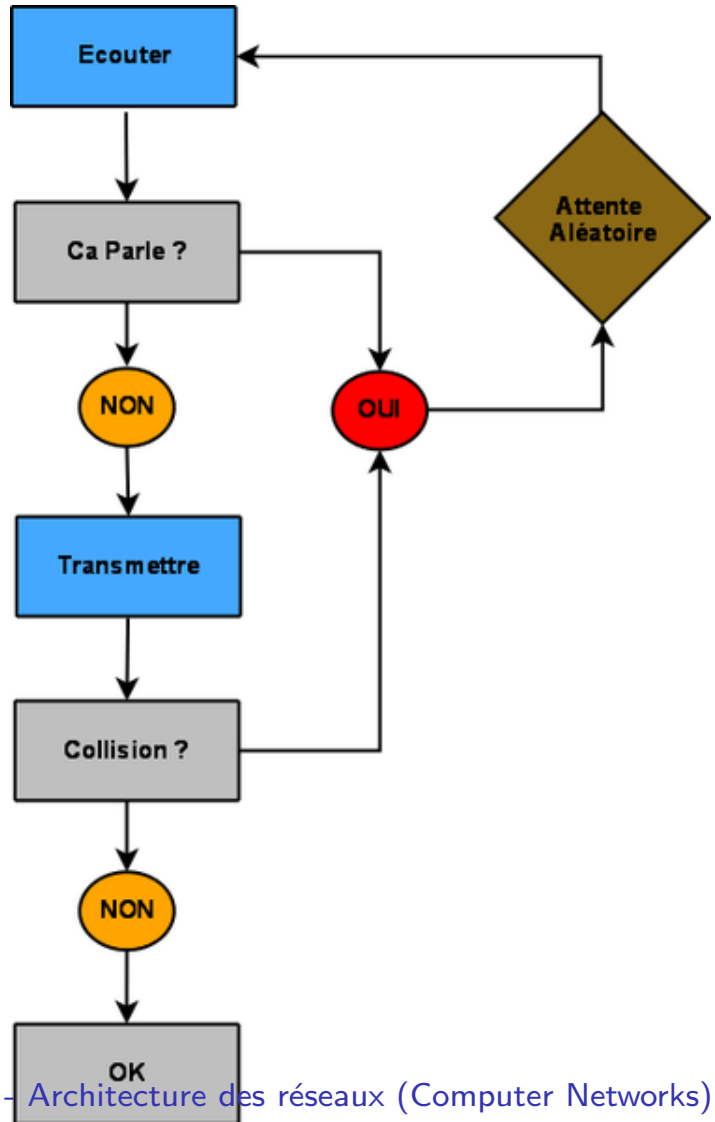
Différentes propriétés d'un canal de communication :

- **simplex**, unidirectionnel (transporte l'information dans un seul sens)
- **half-duplex**, bidirectionnel (dans les deux sens) mais pas simultanément
- **full-duplex**, bidirectionnel simultanément

Accès au médium filaire en l'absence de canal full-duplex

Quand l'équipement n'offre pas un accès *full-duplex*, le protocole **Carrier Sense Multiple Access/Collision Detection** (CSMA/CD) gère le partage de l'accès physique au réseau Ethernet, selon la norme IEEE 802.3.

Aujourd'hui les réseaux locaux sont 100% commutés i.e. les machines communiquent seulement via des *switch* qui utilisent des canaux différents pour émettre/recevoir des données (*full duplex*). **Le problème de collision n'existe plus...**



Architecture TCP/IP – Sommaire

TCP/IP – Histoire

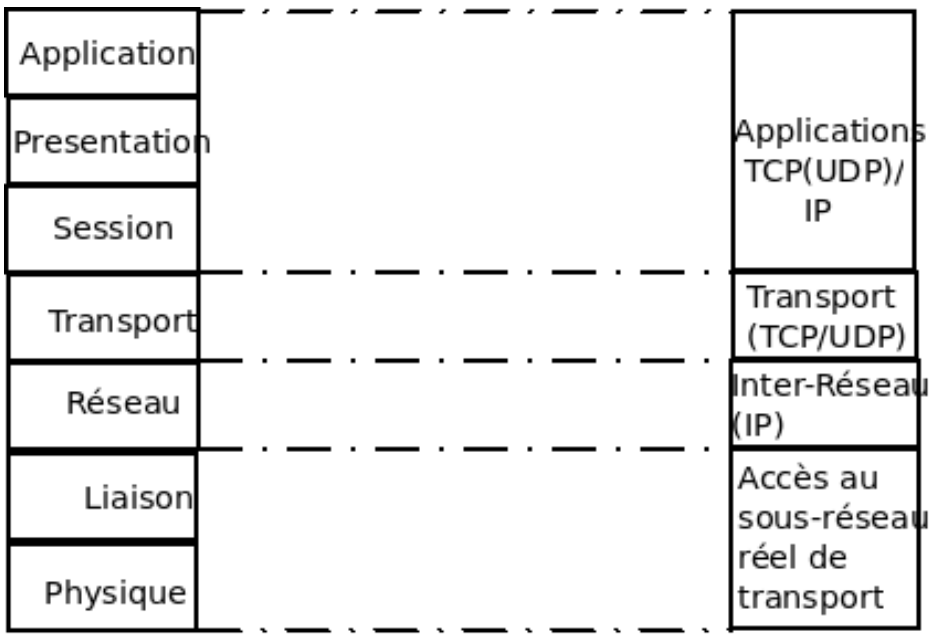
- 1969 : **(D)ARPA du DoD** – 4 noeuds
  (Defense) Advanced Research Project Agency du *Departement Of Defense*
  (deviendra DARPA en 72)
- 1972 : **ARPANET**, ancêtre d'Internet – 40 machines connectées
  Plusieurs réseaux (laboratoires, universités) co-existent dans le monde
  Plusieurs pays décident de les mettre en réseaux : c'est le projet *InterNetwork*, abrégé en **Internet**
- 1977 : Plus de 100 sites connectés
- 1978 : **IPv4 (Internet Protocole version 4)**, naissance d'Internet
- 1980 : Unix inclut la **pile TCP/IP** (Univ. Berkeley)
- 1986 : Backbone NSFnet (56Kpbs) – Dorsale du réseau de la National Science Fundation, liaison Europe/Etats-Unis
- 1995 : **IPng (IP next generation) ou IPv6**

TCP/IP – Intérêts

- **Indépendance** vis-à-vis des constructeurs et OS
- **Gratuité de la documentation** :
  RFC (Request For Comments) – http://abcdrfc.free.fr/
- **Coopération / éthique** sur les projets
- **Simplicité** de mise en oeuvre
- **Beaucoup de services** offerts : mail, news, ftp...

Le modèle OSI et l'architecture TCP/IP

Le modèle OSI compte 7 couches théoriques, l'architecture TCP/IP en définit 2 (une couche Transport et une couche Inter-connexion des réseaux) mais en suppose 2 de plus : Application et Infra-structure.

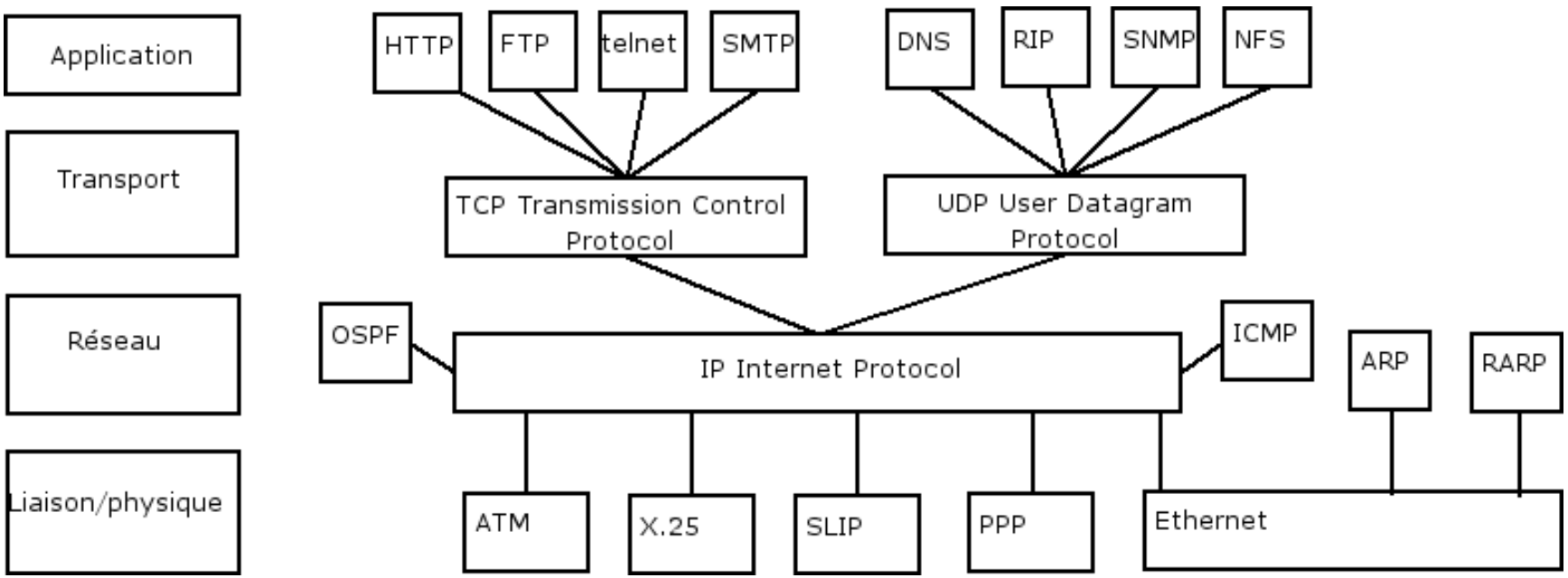


On dit "TCP/IP" avec TCP et IP, des protocoles resp. de Transport et d'Inter-connexion des réseaux. Mais TCP compte une alternative à savoir UDP.

L'architecture TCP/IP

- **Les applications s'appuient sur les services de la couche Transport**
- La **couche Transport gère l'acheminement d'un message de bout en bout**
- La **couche Réseau gère l'acheminement individuel d'un paquet** d'information de ce message
- **Développé au dessus d'un environnement existant**
  - Ne décrit pas de couche physique ni de liaison de données
  - L'utilisation massive de TCP/IP a fait apparaître des réseaux tout IP et la nécessité de disposer de protocoles de liaison point à point (SLIP puis PPP).

Protocoles et applications TCP/IP



Protocoles et applications TCP/IP

- La couche transport (de bout en bout) fournit 2 types de service aux applications
  - En **mode connecté (TCP)**
  - De type **best effort/datagramme (UDP)**
- La couche réseau fournit 1 type de service à la couche transport
  - Mode **non connecté/datagramme (IP)**

Deux modes de services

Deux modes de services peuvent être offerts par une couche pour une transmission

- Service en **mode connecté/orienté connexion**
- Service en **mode non connecté/datagramme/best effort**

Service en mode connecté (orienté connexion)

- **Transfert rendu fiable par l'établissement d'une connexion**
- **Communication en 3 phases**
  - établissement de la connexion
  - transfert de données
  - libération de la connexion
- **Confirmation** (on dit aussi "acquittement" ou **ack***nowledgement* en anglais) de la demande de connexion et de la réception de données

Service en mode non connecté/datagramme/best effort

- Appelé aussi **datagramme** (nom de l'unité de donnée transportée) ou **best effort** en l'absence d'une garantie de délivrance (mode pour le mieux)
- **Communication**
  - par échange de datagrammes indépendants
  - sans connexion
  - sans confirmation

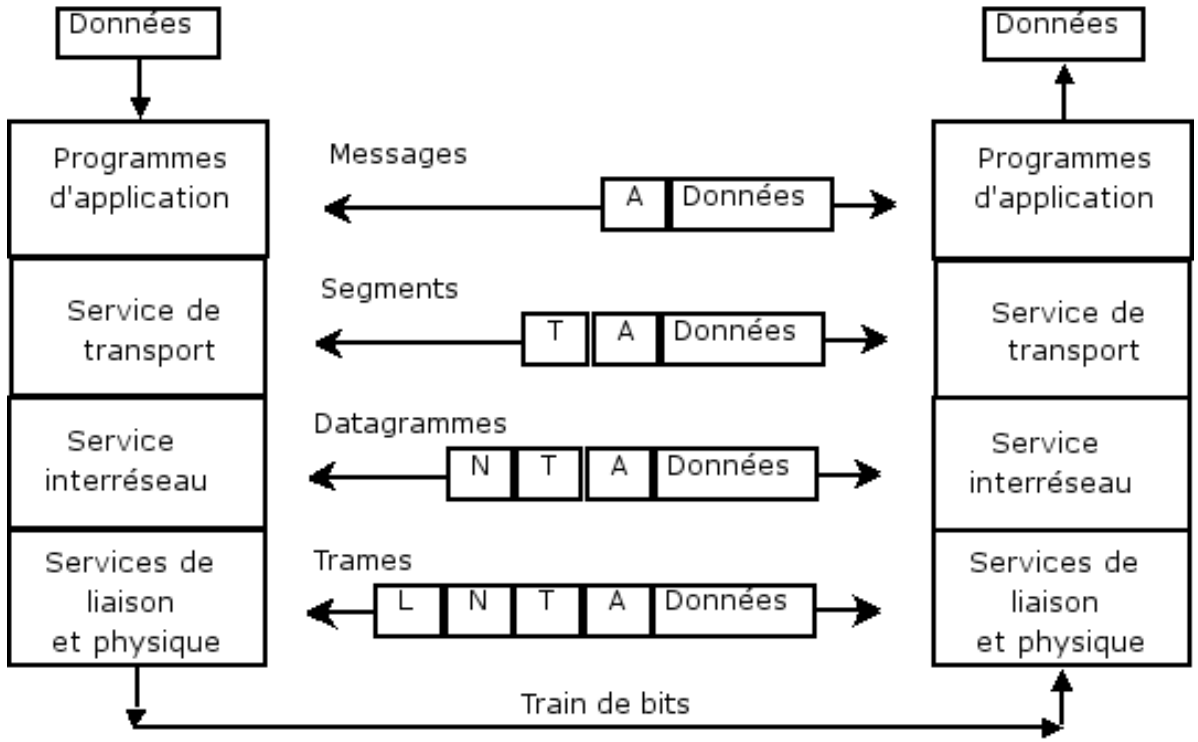
Modes de service – Conclusion

Critères	Orienté connexion	Non connecté
Mise en relation nécessaire	obligatoire	non
Délai de connexion	oui pouvant être important	non car pas de connexion
Allocation de ressources	oui à la connexion	non
Contrôle de flux	oui	non
Séquencement	oui garantie par le réseau	non à la charge du destinataire
Reprise sur incident	oui	non
Résistance à la défaillance	non il faut reconstituer la connexion	oui routage selon l'état du réseau

Modes de service – Conclusion

- Un **service en mode connecté ou non connecté offert par une couche ne dépend pas du support utilisé, mais des protocoles mis en oeuvre par cette couche**
- Définir, pour un réseau, le type de protocole à utiliser, résulte d'un choix essentiellement fondé sur les performances et la qualité de service que l'on désire obtenir.

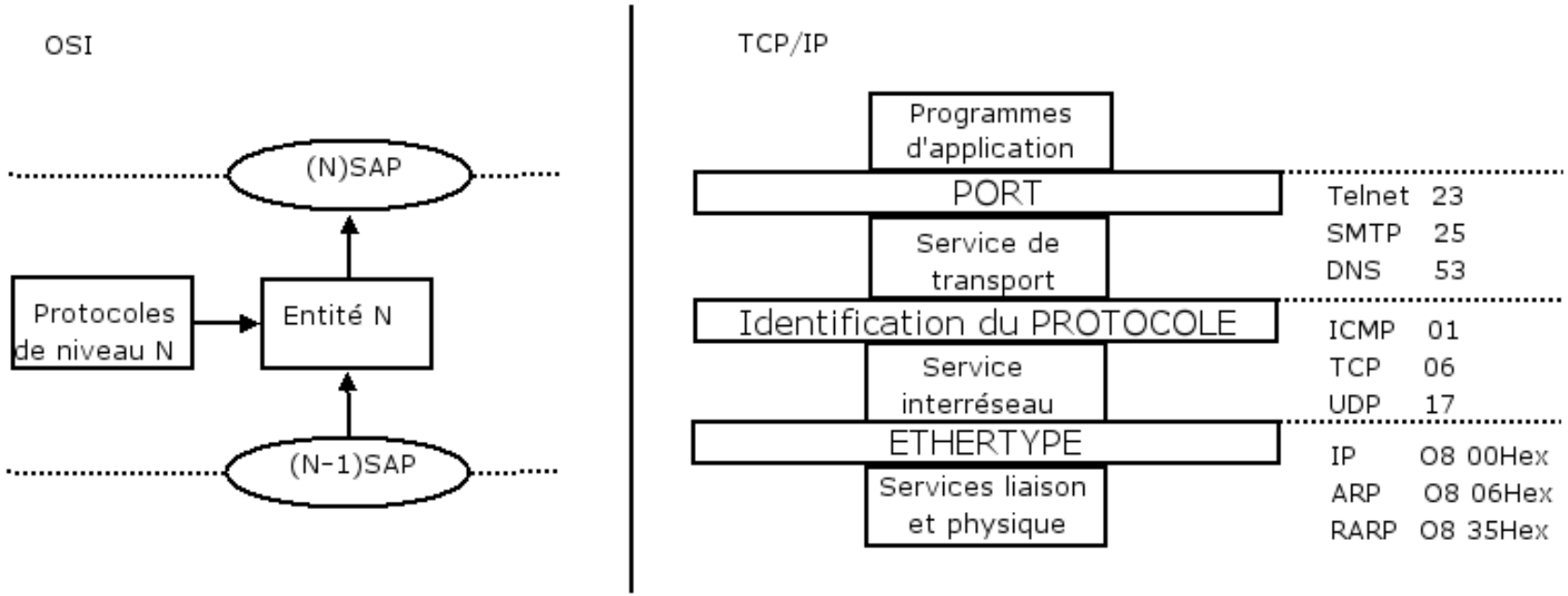
TCP/IP – Encapsulation des données



Différences terminologiques entre OSI et TCP/IP :

- couche transport : OSI(Message) = TCP/IP(Segment)
- et couche réseau : OSI(Paquet) = TCP/IP(Datagramme)

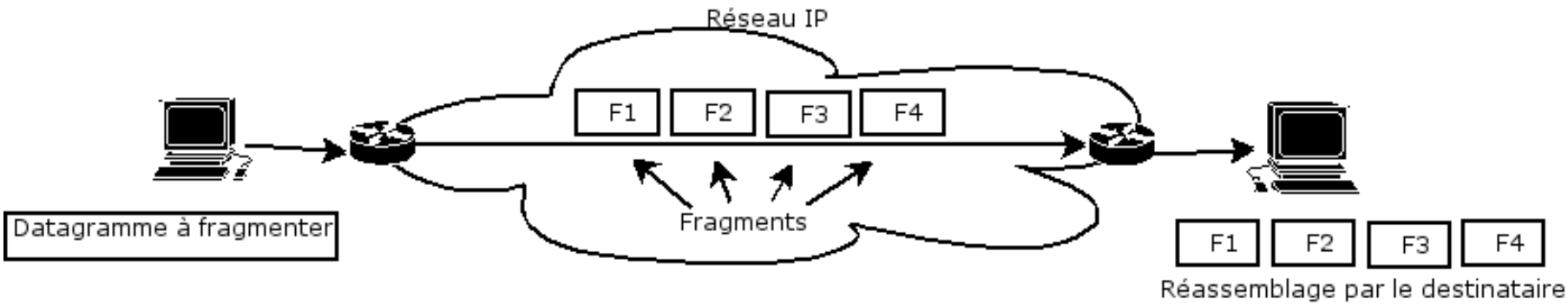
TCP/IP – Identification inter-couches



A l'instar d'ISO avec la notion de SAP (Service Access Point),

- L'**ETHERTYPE dans les trames Ethernet** identifie le protocole du niveau réseau
- L'**identifiant de protocole dans le datagramme IP** désigne le protocole de transport utilisé
- La notion de **PORT dans le segment TCP** détermine l'instance locale de l'application

TCP/IP – Taille maximale des données transférées



MTU (Maximum Transfer Unit) : taille maximale d'un datagramme (en-tête + données) pouvant être transmis en une seule fois (sans risque d'erreur) sur une liaison.
Si le datagramme à transférer est de taille supérieure à la MTU de la liaison, alors l'équipement d'accès devra la fragmenter.
Quelques MTU selon les liaisons :

- IEEE 802.3 Ethernet (i.e. CSMA/CD) : 1500 octets
- IEEE 802.5 Ethernet Token Ring : 1000 o.
- X.25 : 128 o.
- FDDI (Fiber Distributed Data Interface – cable à fibre optique) : 4352 o.

Services de la couche réseau dans le modèle OSI

Quatre fonctions principales :

- assurer **le routage** des paquets à travers un réseau grâce aux routeurs
- assurer **l'interconnexion de réseaux hétérogènes** grâce aux passerelles
- gérer **l'adressage des stations** du réseau
- assurer **le contrôle de congestion** du réseau lorsque le trafic devient trop important

Quizz de synthèse

- Définir la notion OSI de SAP dans le contexte d'une architecture TCP/IP.
- Quelles incidences a la MTU d'un réseau sur le transfert d'un paquet ?

Adressage – Sommaire

Type d'adressage

Problème

Comment désigner de manière unique et non ambiguë un destinataire ?

Cela dépend de la faciliter que l'on a pour le trouver...

- Si le destinataire est local, on "n'a pas besoin" de le chercher. Un identifiant **unique et absolu** suffit
  - Ex : adresse physique Ethernet (MAC)
- Si le destinataire est distant, il faut le trouver. Un identifiant **hiérarchique** est requis
  - Ex : numéro téléphone, adresse postale, adresse logique IP (différentes politiques de structuration)
  - Politique de structuration des numéros de tel : <indicatif de pays> <code de ville/zone> <numéro de téléphone> avec 33 / 2 / 40 30 60 90

Adressage plat/absolu

- pour **identifier localement un matériel au niveau physique**
- ☺ Avantages : identifiant universel unique
- ☹ Inconvénients : **peu d'information de localisation**, difficile de retrouver un correspondant

Adressage hiérarchique

- pour **router "facilement"** des données entre les réseaux
- Et avoir une **organisation d'un réseau indépendante de celle qui découle de la liaison physique** des machines
- En cas de panne matériel ou de déplacement géographique, **cela évite de mettre à jour les tables de routage** de chaque machine d'un réseau
- ☺ Avantages : adapté aux grands réseaux et à la localisation
- ☹ Inconvénients : un changement de localisation entraîne des changements d'adresses et/ou de noms d'hôtes et des systèmes de redirection

Note : Une machine possède **autant d'adresses logiques que de réseaux auxquels elle est connectée** ; et par conséquent autant de cartes réseaux (référencées dans la machine par un identifiant d'interface)

Différents modes de diffusion

- *unicast*, connexion réseau point à point, un hôte vers un (seul) autre hôte
- *multicast*, un émetteur (source unique) vers un groupe de récepteurs
- *broadcast*, un émetteur unique vers l'ensemble des récepteurs

L'adressage physique MAC (Medium Access Control)

- **Adresse absolue : une adresse MAC identifie une machine (ordinateur, routeur) de manière unique au niveau liaison**
- Constituée de **48 bits (6 octets/lots de 8 bits)** et représentée sous **forme hexadécimale avec un double point séparant les octets** (12 caractères hexa). Un caractère est codé sur 4 bits (et compte 2^4 valeurs, soient les 16 possibles de l'hexa).
- Exemple : 5E:FF:56:A2:AF:15

Unicité des adresses MAC

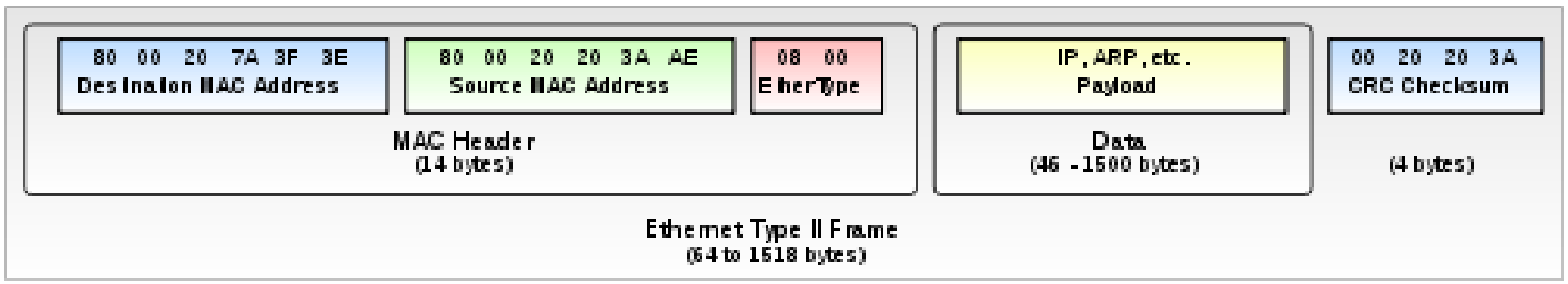
Pour garantir l'unicité des adresses **chaque carte réseau construite a sa propre adresse MAC** .
Les 3 1ers octets sont spécifiques à un constructeur (attribué par l'IEEE)

Entité	**Préfixe (en hexa)**
IBM	08:00:5a
CISCO	00:00:0c
3COM	02:60:8c, 00:A0:24, 08:00:02

Adresse MAC réservée

Adresse de diffusion/broadcast Pour atteindre toutes les machines connectées sur la liaison courante on utilise l'adresse $FF:FF:FF:FF:FF:FF$ (tous les bits à 1)

Format d'en-tête d'une trame Ethernet II



Credits:commons.wikimedia.org

- 6 octets par adresse MAC (destination puis source)
- 2 octets pour l'Ethertype (13e et 14e octets)
- Taille des données spécifique à la liaison. Voir MTU..

	Ethertype
IP	08:00
ARP	08:06
RARP	08:35

Code du protocole encapsulé dans la trame (en hexa)

L'adressage IPv4 (Internet Protocol version 4)

- La **forme binaire** (chaîne de 32 bits) n'étant pas facile à mémoriser, on a l'habitude d'utiliser une **forme décimale pointée** du type x1.x2.x3.x4 avec chaque x*i* représentant un octet (8 bits)
- Exemple d'adresse IPv4 : 172.16.15.3
- Une adresse IP se décompose en 2 parties
  - **Identifiant réseau** sur lequel se situe la machine
  - **Identifiant machine** (aussi appelée partie matérielle)

Comment indiquer au système où finit la partie réseau et où commence la partie machine ?

Masque de (sous-)réseau, notation décimal pointé et CIDR

Principe

Chaque machine identifie les bits de son adresse IP réservés à l'ID réseau grâche au **masque de (sous-)réseau (net mask)**

Définissable sous la forme d'une adresse IP en **décimal pointé**

- **Chaque bit du masque correspondant à ID-Réseau est positionné à 1 et chaque bit correspondant à ID-Machine est positionné à 0**
- Ex : 255.255.255.0 ou 255.255.254.0 (le 3e octet équivaut à 11111110 en binaire) ou 255.255.255.64 (le 4e octet équivaut à 1000000 en binaire)

La **notation CIDR (*Classeless Inter Domain Routing*)**

- **indique le nombre de bits de poids fort pour l'ID-réseau a.b.c.d/n**
- Ex : 192.168.123.201/24 ou 192.168.123.201/23 ou 192.168.123.201/25

Ici vous remarquerez qu'il y a une correspondance entre les exemples de masques exprimés en décimal pointé et en CIDR...

Comment savoir si une machine appartient à mon réseau ?

Principe

1. *En opérant un* **et logique** *entre mon masque réseau et mon adresse IP sur ce réseau, j'obtiens l'adresse de mon réseau.*
2. *En opérant un* **et logique** *entre mon masque réseau et l'adresse d'une autre machine, j'obtiens encore une adresse de réseau.*
3. *Si les deux adresses de réseau sont les mêmes, ça veut dire que les deux machines appartiennent bien au même réseau.*

Ex 192.168.192.168/18 et 192.168.250.250/18, sur le même réseau ?

- /18 = 8+8+2 cela concerne le 3e octet
- Les deux premiers octets sont identiques
- 192d = 1100 0000b et 250d = 1111 1010b
- les 2 bits manquants sont aussi identiques. Ils sont sur le même réseau.

Adresses spéciales

- **Adresse réseau** : identifie un réseau
  Tous les bits de la partie machine de l'adresse logique ont la valeur 0
  e.g. 172.16.0.0/16
- **Adresse de diffusion (Broadcast)**
  - **Limitée** : adresse toutes les machines du réseau local de la machine où vous êtes connecté
    Tous les bits sont à 1 i.e. 255.255.255.255
  - **Dirigée** : adresse toutes les machines d'un réseau local donné
    Tous les bits de la partie machine ont la valeur 1
    e.g. 172.16.255.255/16

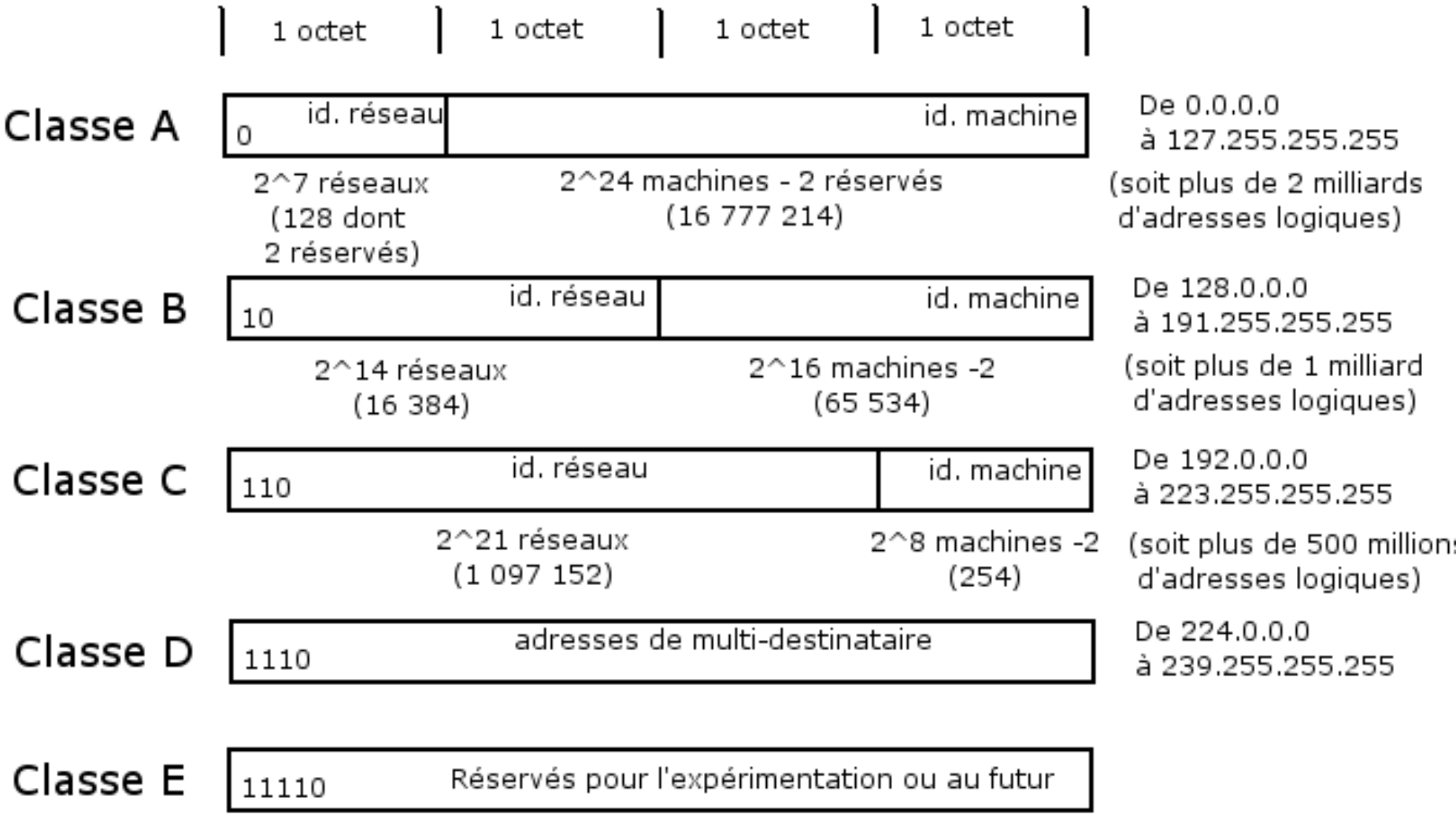
Cinq classes d'adresses

- Historiquement, "on" avait décidé qu'il y aurait sur l'Internet des **classes** de réseaux, **chacune avec une capacité prédéfinie de machines adressables**.
- Par voie de fait, le **nombre de réseaux disponibles par classe lui aussi fixé** était inversement proportionnel au nombre de machines adressables dans un réseau de cette classe. Sur 32 bits que compte une adresse IP, il ne pouvait y avoir que 2^8 réseaux pouvant contenir $2^{24} - 2$ machines par exemple.
- Les classes **se distinguaient à partir des premiers bits** (ou de la valeur décimale) **du premier octet** de l'adresse IP.
- A chacune des classes correspondait **un masque lui aussi prédéfini** qui **séparait la partie ID-réseau et ID-machine à la jonction entre deux octets** de l'adresse IP.

Cinq classes d'adresses

- La notion de classe a été **abandonnée au profit de la notion CIDR** (*Class-less..*) car elle ne permettait pas une exploitation optimale du format IP.
- Le principe CIDR permet de **séparer un ID-réseau d'un ID-machine quasiment à chaque bit** d'une adresse IP et donc au final cela permet de définir davantage de réseaux qu'avec la notion de classe.
- La notion de classe est présentée ici car nos systèmes (d'exploitation) en gardent souvent trace...

Cinq classes d'adresses



Cinq classes d'adresses

- Les classes A, B et C servent à adresser **des réseaux de différentes tailles**
- Les classes **A et B sont totalement saturées** et plus aucune classe de ce type n'est disponible
  E.g. de classe A : DoD, MIT (Massachusetts Institute of Technology)
- La classe **D définit des adresses multi-destinataires** correspondant à des groupes d'ordinateurs
  (adresses IP multicast)
- La classe **E avait été prévue initialement pour les évolutions futures** d'Internet
  Dans les faits, elle a été très peu utile à cause de la saturation rapide des classes A, B et C.

Masque et classes

- Classe A : <IP classe A> et 255.0.0.0 ou <IP classe A>/8
- Classe B : <IP classe B> et 255.255.0.0 ou <IP classe B>/16
- Classe C : <IP classe C> et 255.255.255.0 ou <IP classe C>/24

Adresses réservées

2 adresses réservées au sein de la classe A

- Adresse **d'initialisation : 0.0.0.0**
  - Lors du lancement d'une machine en attente d'une réponse à sa demande d'attribution d'adresse
  - Dans les routeurs désigne la route par défaut
- Adresse **locale (localhost) ou de bouclage (loopback) : 127.x.x.x** (e.g. : 127.0.0.1)
  - Permet de s'auto-désigner
  - Utilisée pour effectuer des tests ou des échanges de données entre applications sur une même machine

Adresses spéciales

- **Adresses publiques/privées**
  - Pas tous les réseaux ont un besoin d'interconnexion via un réseau publique e.g. une entreprise et son intranet
  - Pour éviter une anarchie, IANA a réservé certaines plages d'adresses dans chaque classe
    En classe A : 1 réseau (10.0.0.0) ; B : 16 (de 172.16.0.0 à 172.31.0.0) ; C : 256 (de 192.168.0.0 à 192.168.255.0)
  - Un **NAT (Network Address Translator)** peut être utilisé pour mettre en correspondance un réseau privé et un réseau publique

Plan d'adressage - exemple

Soit l'adresse IP suivante 192.168.123.202/23, quid du reste ?

- Quelle est la valeur du masque en décimal pointé ?
- Quelle est l'adresse réseau ? L'adresse de diffusion/broadcast ?
- Combien de machines peuvent être adressées sur ce réseau ?
- Quelle est la plage d'adresse IP sur ce réseau ?

Réponses... ?

Plan d'adressage - exemple

Réponses (sans le détail des calculs) :

Masque de Sous-Reseau = 255.255.254.0

Masque Inverse (Wildcard) = 0.0.1.255

Adresse Reseau = 192.168.122.0

Adresse Broadcast = 192.168.123.255

Nombre de Machines = 510

@IP Premiere machine = 192.168.122.1

@IP Derniere machine = 192.168.123.254

Sortie console de la commande ifconfig

`ifconfig` (sous linux) : connaître les interfaces réseaux (et leurs identifiants) présentes sur une machine, savoir celles qui sont configurées et les configurer

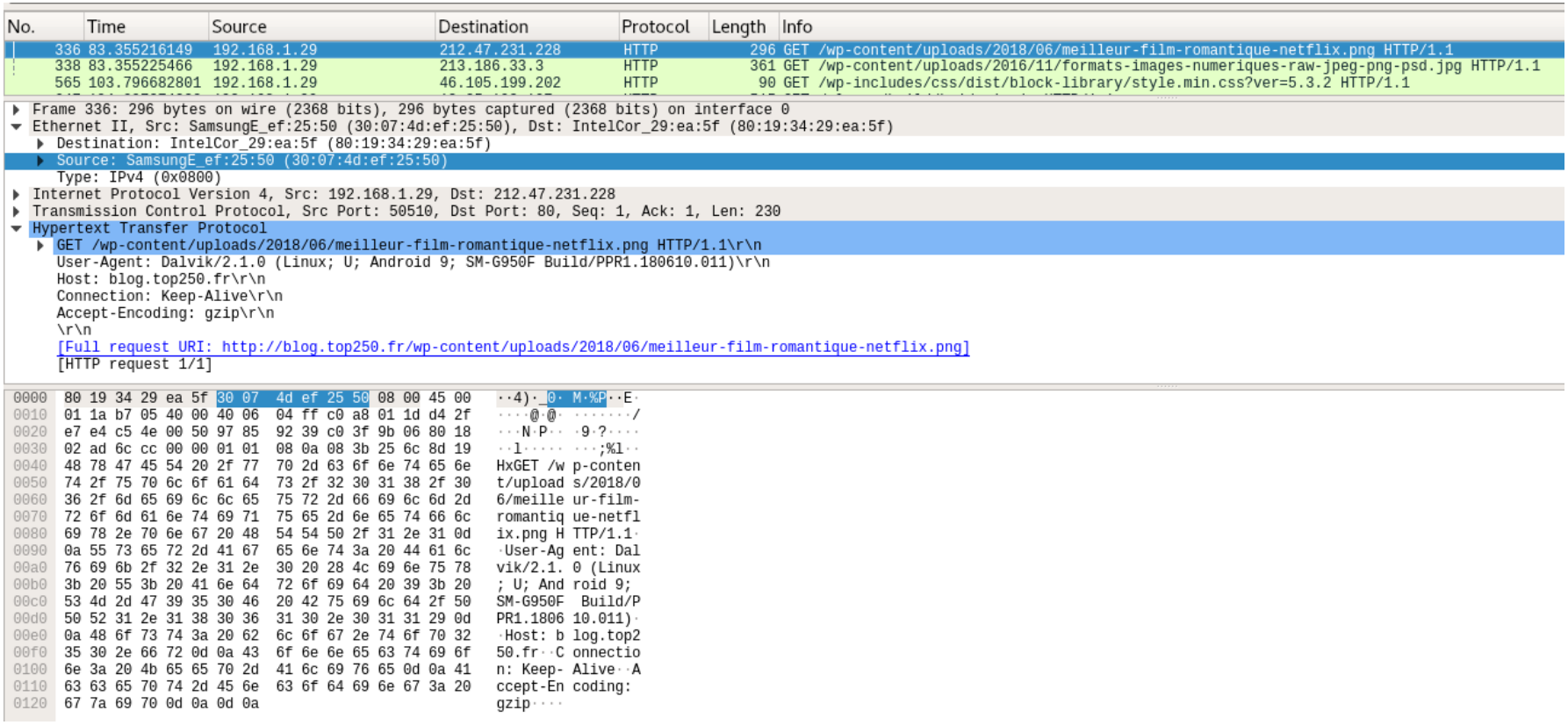
```
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 34:64:a9:d4:cb:36  txqueuelen 1000  (Ethernet)
        RX packets 1594749  bytes 2261487441 (2.2 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 596319  bytes 367641874 (367.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xd0700000-d0720000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Boucle locale)
        RX packets 235844  bytes 203813235 (203.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 235844  bytes 203813235 (203.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.18  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f988:ac84:c757:703e  prefixlen 64  scopeid 0x20<link>
        ether 80:19:34:29:5fs:ea txqueuelen 1000  (Ethernet)
        RX packets 3166365  bytes 3509196664 (3.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1952486  bytes 980678646 (980.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Sortie console de la commande "ip a"

`ip a` (sous linux) : alternative à *ifconfig* qui permet une configuration "aux petits oignons"

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 34:64:a9:d4:cb:36 brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 80:19:34:29:5f:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.18/24 brd 192.168.0.255 scope global dynamic noprefixroute wlo1
       valid_lft 79195sec preferred_lft 79195sec
    inet6 fe80::f988:ac84:c757:703e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Aperçu d'une trame Ethernet dans Wireshark



Source de la capture : `https://wiki.wireshark.org/SampleCaptures`

Quizz de synthèse

- Quelles différences majeures existent ils entre une adresse MAC et une adresse IPv4?
- Comment peut on préciser quelle est la partie réseau d'une adresse IP ?

Le protocole réseau IPv4 – Sommaire

IP – Objectifs et fonctions

Protocole de niveau paquet (réseau) actuellement utilisé sur l'Internet ; majoritairement dans sa version IPv4 mais bientôt remplacée par IPv6

Interconnexion de réseaux hétérogènes

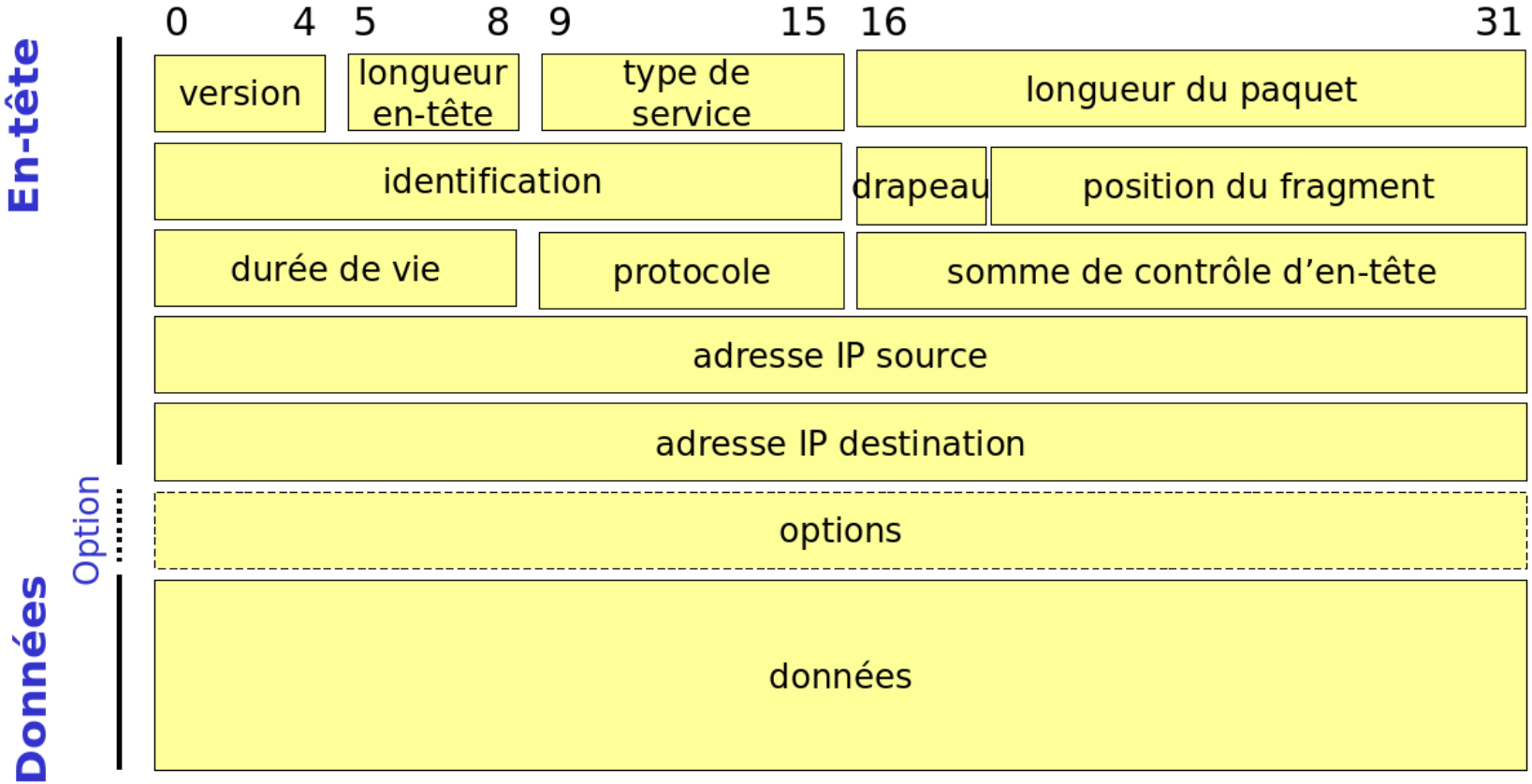
- **Adressage universel** (interconnexion de n'importe quel type d'hote)
  - hiérarchique à deux niveaux (réseau–hôte)
  - unicité garantie par un organisme fournisseur : IANA (Internet Assigned Numbers Authority)
- Capable de **transporter plusieurs protocoles** (un champ indique le protocole transporté)
- **Adaptation au réseau physique sous-jacent** fragmentation / réassemblage selon capacités d'emport de la liaison (MTU)

IP – Objectifs et fonctions

Qualité de Service (QoS) de type **Best effort** (au mieux)

- **Transmission non fiable : Service en mode sans connexion et sans acquitement des données**
  - indépendance des datagrammes, possibilité de perte de paquet, de duplication, de livraison dans le désordre et de congestion des routeurs
  - garantie d'acheminement gérée par couche supérieure
  - un TTL (Time To Live) pour la prévention de la congestion
- Communication **avec faible contrôle d'erreurs**
  - Si erreur détectée, tentative d'envoie d'un paquet ICMP
  - La qualité du service laissée à la charge de couche supérieure

Format d'un datagramme IPv4



- La taille des datagrammes IP ne doit pas excéder 65536 octets
- Taille de l'en-tête = 20 octets (i.e. 5 * 4 octets ou 5 * 32 bits)

Champs de l'en-tête IPv4

- Version : 4 bits
  - Format du protocole IP ;
  - Permet la **cohabitation de IPv4 (0100) et IPv6 (0110)** sur un même réseau
- Longueur de l'en-tête (IHL – Internet Header Length) : 4 bits
  - **En mots de 32 bits** (min 5, max 15)
  - **Permet de détecter la présence du champ Option**
- **Type de service (TOS)** : 8 bits

priorité.délai.débit.fiabilité.coût.réservé

7	6	5	4	3	2	1	0
priorité			TOS				0

  - E.g. SMTP, envoi de données : 000.1.0.0.0.0 (minimise le délai)
    SMTP, contrôle/commande : 000.0.1.0.0.0 (maximise le débit)
  - Défini dans RFC 791 ; depuis révisé dans RFC 1812
- **Taille en octets du datagramme (en-tête + données)** : 16 bits
  - non fixe mais limité à 65536 o.

Champs de l'en-tête IPv4

- Identification, 16 bits
  - Attribué aléatoirement par la source
  - **Indique à quel datagramme appartient le fragment** (utilisé avec l'adresse IP source par le destinataire)
- Drapeau (Flag), 3 bits : permet de **savoir si le datagramme est fragmenté**
  - 1er bit non utilisé ;
  - 2e bit DF (Don't Fragment) utilisé quand l'extrémité est incapable de réassembler ; un routeur détruit un tel paquet s'il ne peut le transférer
  - 3e bit MF (More Fragment) utilisé pour fragments de 1 à $n-1$
- Position du fragment (Offset), 13 bits
  - **Position** dans datagramme d'origine **en multiple de 8 octets** ; i.e. quantité de données déjà transmises
  - Tous les fragments ont une taille multiple de 8 octets sauf le dernier

Champs de l'en-tête IPv4

- Durée de vie (TTL – Time To Live), 8 bits
  - **Limite la présence sur le réseau**
  - Décrémentée à chaque routeur et retirée à 0
- Protocole, 8 bits

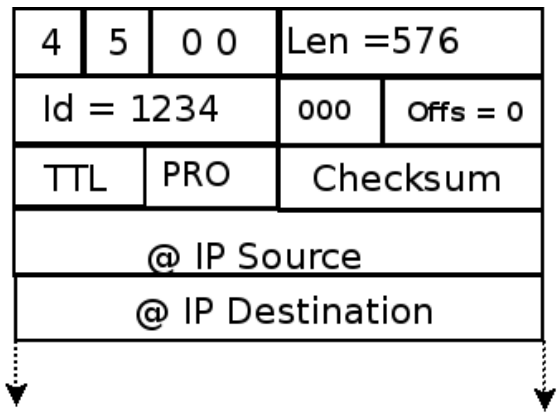
Spécifie protocole de niveau transport à l'origine de l'émission pour être traité par même protocole à la réception

TCP	6
UDP	16
ICMP	1

- Somme de contrôle de l'en-tête (Checksum), 16 bits
  - **Recalculée pour chaque intermédiaire** ; paquet **rejeté si erreur**
  - **Données vérifiées à la couche transport** supérieure
- **Adresses IP** source et destination, 32 bits chacune
- Options
  - Contraintes d'acheminement du datagramme
  - **Bits de bourrage** pour compléter jusqu'à 32 bits

Fragmentation d'un datagramme IPv4

Soit un paquet IP de 576 octets à acheminer sur un réseau X.25 (rappel : MTU(X.25) = 128 o. dont 20o. en-tête + 108 o. de charge effective



- Sachant qu'un fragment doit avoir une taille de données multiple de 8, quelle taille maximale de donnée aura un fragment ?
- Combien de fragments et la taille totale de chacun (Champ Len) ?
- Que met on dans les champs position et flags de chaque paquet-fragment ?

Sachant qu'un fragment doit avoir une taille de données multiple de 8, quelle taille maximale de donnée aura un fragment ?

- 108 non divisible par 8 ; le plus grand nombre inférieur à 108 et divisible par 8 est 104

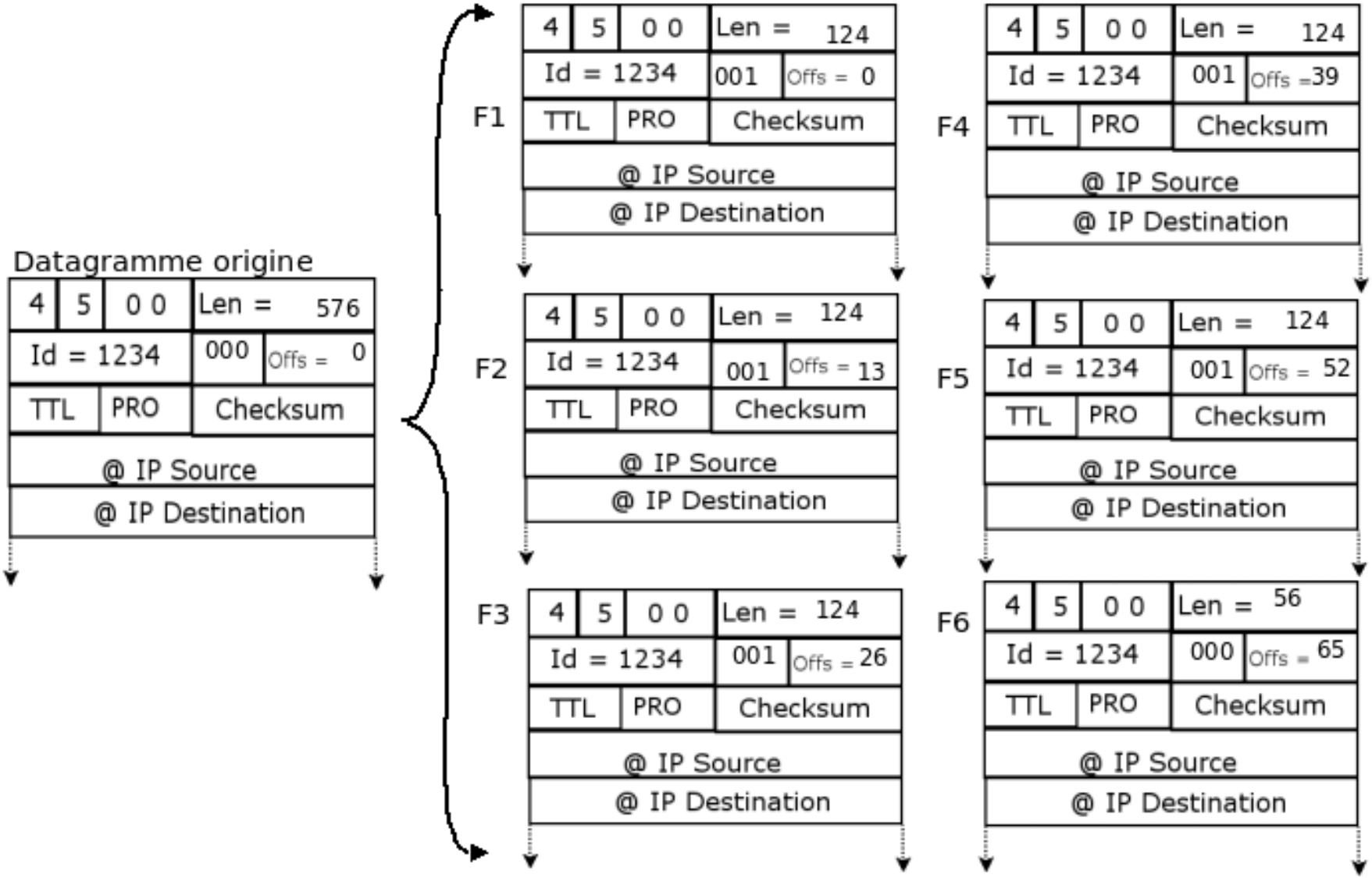
Combien de fragments et la taille totale de chacun (champ Len) ?

- Charge effective que l'on veut transporter est de (576 - 20 o. en-tête) / 104 = 5,34 (en fait 5 * 104 + 36)
- Ce qui fait 6 paquets-fragments auxquels on rajoute à chacun les 20 o. d'en-tête
- Respectivement Longueur (Len) = 124 pour les 5 premiers Fragments et 56 pour le dernier

Que met on dans les champs position et flags de chaque paquet-fragment ?

- Les positions (Offs) sont 0 pour le 1er, 104/8=13 pour 2ème, 2*(104/8) = 26 pour 3ème ...
- Flag MF(001) sauf pour le dernier (000)

Fragmentation d'un datagramme IPv4



Note : Len et Offs donnés ici en décimal pour faciliter la lecture

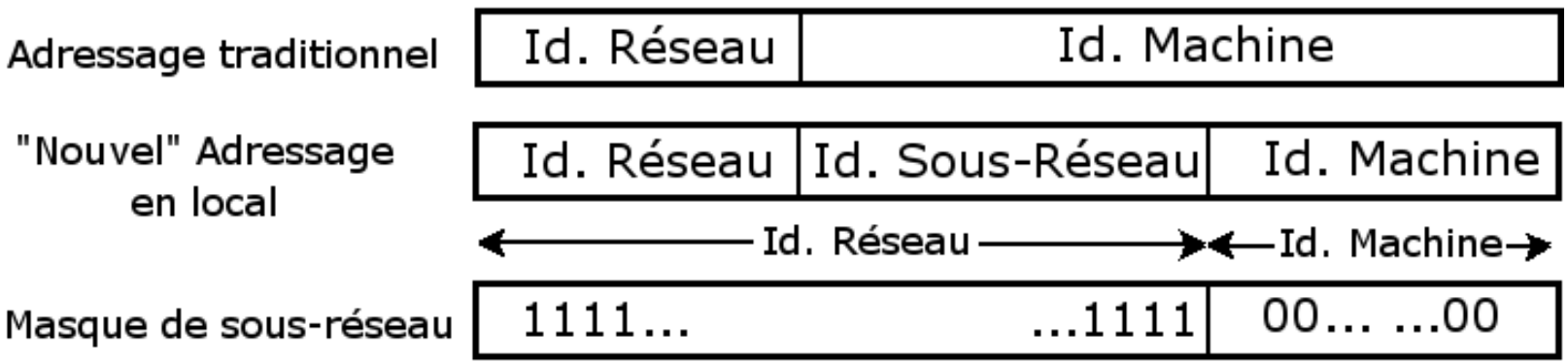
Découper en sous-réseaux

Problème

Une seule adresse réseau attribuée et besoin d'en considérer plusieurs pour des raisons de sécurité, répartition du trafic, cohérence (Prof, Etudiant, etc.)

Solution

Utilisation de bits de poids forts de l'identifiant machine *pour représenter des sous-réseaux*



Exemple de découpage en sous-réseaux

On souhaite découper le réseau 192.168.1.0 (Classe C) en 4 sous-réseaux

- Ad. Diffusion = 192.168.1.255
- Masque de réseau = 255.255.255.0 aussi noté 192.168.1.0/24
- Nombre d'adresses matérielles = 254 réservées (réseau et diffusion)

Pour coder 4 sous-réseaux, il faut 2 bits : 00, 01, 10, 11

- Masque de sous-réseau = 255d.255d.255d.11000000b i.e. 255d.255d.255d.192d ou encore 192.168.1.0/26
- Adresses matérielles = 2^6 adresses logiques - 2 = 62
- Nombre total de matériels 4 * 62 = 248

Sous-réseaux	**Nb. de machines**	**Zone d'adressage matériel**	**Ad. réseau**	**Ad. de diffusion**
Sr1	62	.1 -> .62	.0	.63
Sr2	62	.65 -> .126	.64	.127
Sr3	62	.129 -> .190	.128	.191
Sr4	62	.193 -> .254	.192	.255

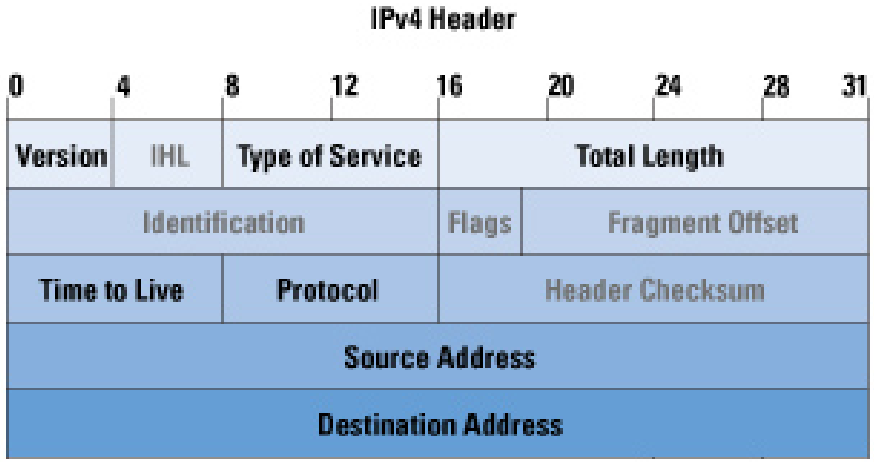
Besoin d'un nouveau protocole ?

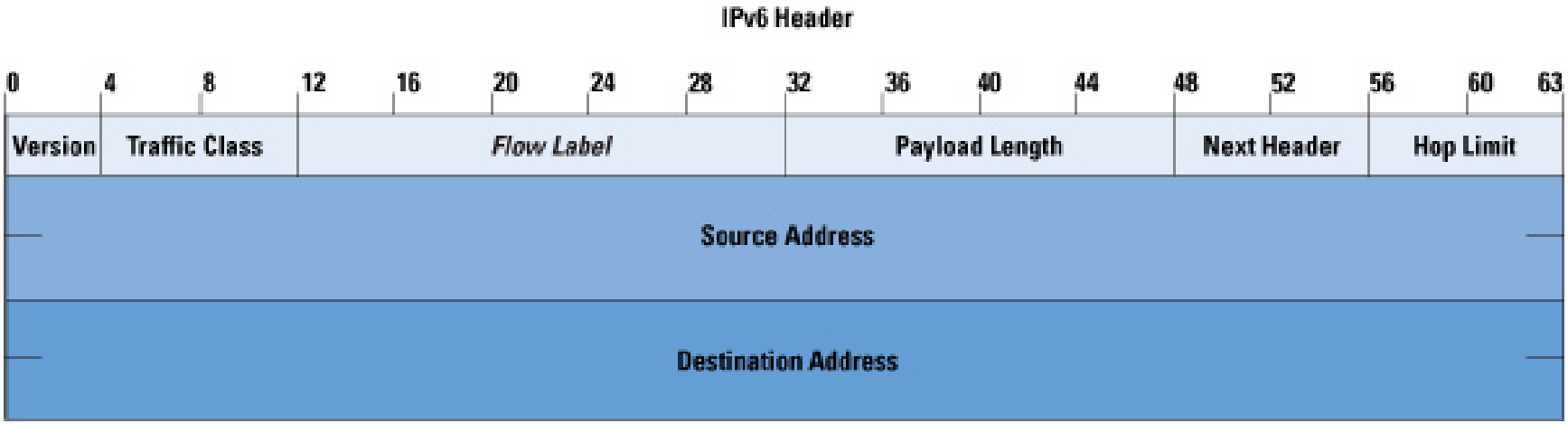
- **Epuisement des adresses IPv4** :
  "Les quatre principaux opérateurs français (Bouygues Telecom, Free, Orange, SFR) ont déjà affecté entre environ 94% et 99% des adresses IPv4 qu'ils possèdent, à fin juin 2019." [3]
  - **NAT (traduction d'adresses privées/publique) : solution à court terme NAT mais coût de performance**
- **Explosion de la taille des tables de routage**
  - **CIDR, solution partielle qui fait disparaître les classes d'adresses**, autorise l'agrégation d'adresses de réseaux contigus en un seul préfixe, organise géographiquement l'affectation des adresses
- **Offre pauvre de services**
  - Ne prend pas en charge en natif : QoS, sécurité, mobilité

[3] https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html

Le protocole réseau IPv6 – Sommaire

Structure du datagramme IPv6 vs IPv4





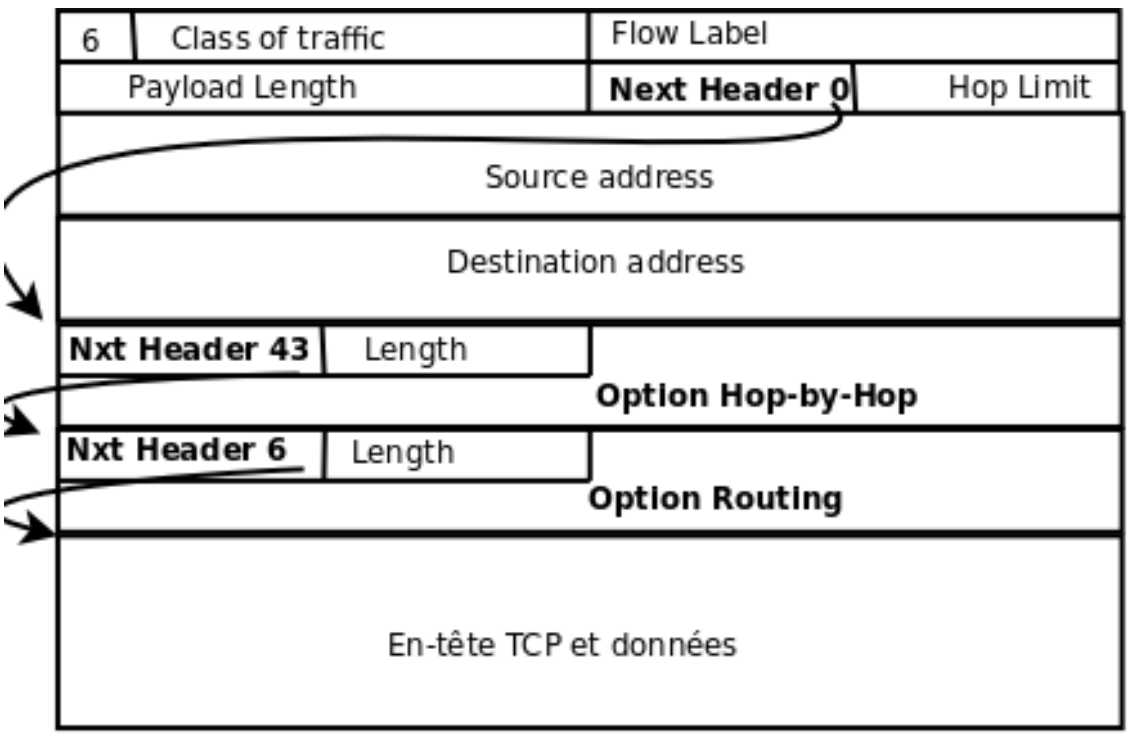
Principales caractéristiques d'IPv6 vs IPv4

IPng (Internet Protocole next generation) – IPv6

- **Espace d'adressage étendu** 128 bits au lieu de 32
  (contre les 4 milliards 300 millions @IPv4 on aura désormais 667 millions d'IPv6 pour chaque millimètre carré de surface terrestre)
- **En-tête simplifié du paquet** (taille figée et moins de champs)
  autorisant un routage plus efficace
- **Longueur constante d'en-tête** 40o
  suppression du champ longueur d'en-tête
- **Sécurité accrue** en incluant mécanismes d'authentification, de confidentialité, et d'intégrité (Protocole IPSec)
- **Amélioration des aspects de diffusion multicast**
- Support élargi pour les **protocoles IP mobiles**

- Mécanisme de **découverte de MTU optimale**
  fragmentation/réassemblage seulement réalisée par source/destinataire ; suppression des champs de fragmentation (ID, Flags, Offset)
- Mécanisme de **contrôle TCP jugé suffisant**
  suppression du champ checksum
- Champ **TOS remplacé par deux champs classe de trafic et identification de flux**
  initialisé par source, similaire à un numéro de circuit virtuel, routage plus efficace (commutation de niveau 3)
- Système d'**extensions d'en-tête** à la place d'un champ d'options
- Champ longueur totale remplacée par **taille données transportées** (car l'en-tête est de longueur fixe désormais) ; inclut la taille des extensions
- Champ **Protocole transformé en identifiant du type du prochain en-tête ou du protocole transporté**
- Champ **TTL remplacé par compteur de sauts** (positionné par la source, par défaut à 64)

Le chaînage des options/extensions d'en-tête



- 0, option, Hop-by-Hop
- 4, protocole, Ipv4
- 6, protocole, TCP
- 17, protocole, UDP
- 43, option, Routing
- 44, option, Fragment
- 50, option, IPSec (ESP Payload)
- 51, option, IPSec (authentification)
- 58, Protocole, ICMP
- 59, , No Next Header

Le chaînage des options/extensions d'en-tête

Les extensions d'en-têtes remplacent les option d'IPv4
Pour un traitement efficace par les routeurs : ordre prédéfini, taille en mots de 64 bits, aucune traitée par le routeur sauf le Hop-by-Hop
Quelques extensions

Hop-by-Hop (de proche en proche) : la seule lue par les routeurs intermédiaires, indique si celui-ci doit traité ou non le contenu

Routing (routage) : spécifie le mode d'acheminement (libre pour chaque routeur ou liste de routeurs initialement définie)

Fragmentation : pour les applications qui transmettent des données de taille importante et qui pour des raisons d'efficacité utilisent un Transport UDP (exemple NFS) ; similaire au mécanisme d'IPv4

Destination : gestion des destinataires mobiles en associant une adresse locale sur un réseau d'accueil à une adresse principale

Format des adresses IPv6

Adressage hierarchique en 3 parties :

- 48 bits : topologie publique, agrégation hiérarchique de préfixe décrivant la connectivité du site
- 16 bits : topologie locale du site
- 64 bits : identifiant unique au monde de chaque interface

Notation des adresses IPv6

- Base hexadécimale
- 8 * 16 bits (8 mots)
- Séparateur ":"
- Exemple IPv6 globale :
  FE00:0000:0000:0123:4567:0000:0000:0DEF
- Simplification 1 : on enlève les zéros non significatifs
  FE00:0:0:0123:4567:0:0:0DEF
- Simplification 2 : on enlève les zeros au début de chaque mot
  FE00:::123:4567:::DEF
- Notation CIDR possible en exprimant la longueur du préfixe en bits
  FE0C:DA98/32, FE0C:DA98:0:0/64 ou encore FE0C:DA98::/64

Portée des adresses IPv6

La notion de broadcast disparait car trop pénalisant en terme de performance réseau au profit d'une généralisation du multicast
La portée d'une adresse IPv6 consiste en son domaine de validité et d'unicité.
3 types d'envoi :

- **unicast** "individuel" (dont loopback, link-local) i.e. une interface
- **multicast** "diffusion groupée" (FF00::/8) ensemble d'interfaces distinctes dont la localisation n'est pas nécessairement dans le même réseau physique ; les bits 13 à 16 déterminent la portée (local, liaison, organisation ou global)
- **anycast** "à la cantonade" ensemble d'interfaces partageant le même préfixe ; mais datagramme délivré seulement au noeud le plus proche du groupe

Adresses spécifiques IPv6

adresse de liaison locale (link-local) pour la gestion du réseau, fe80::/10 adresse sur la liaison locale, auto-assignable calculée à partir de l'adresse MAC

adresse non spécifiée lors de l'initialisation), ::/128, correspond à 0.0.0.0 d'IPv4

adresse de bouclage (ou loopback) dite de localhost, validité limitée à la machine, ::1/128, correspond à 127.0.0.1 d'IPv4

adresse de site local (privée) FEC0::10 correspondent aux adresses privées IPv4 de type 10.0.0.0

Passage d'IPv4 à IPv6

Différentes solutions assurent la cohabitation

- **Double implémentation des protocoles** au sein du même équipement
- **IPv4 mappée** pour permettre à des applications IPv6 de fonctionner sur un réseau IPv4 (i.e. entre machines IPv4)
  ::FFFF:86CE:0A12 équivalent à ::FFFF:134.206.10.18
- **IPv4 compatible** pour permettre à deux machines IPv6 de communiquer à travers un réseau IPv4 : encapsulation des paquets IPv6 d'adresses : :a.b.c.d dans des paquets IPv4 d'adresse a.b.c.d)
  ::86CE:0A12 équivalent à ::134.206.10.18

Conclusion

Bien que systèmes d'exploitation et équipements supportent IPv6, utilisation du protocole non universelle

- Coûts liés au passage d'IPv4 à IPv6 : il faut acheter ces nouveaux logiciels et matériels
- Utilisateurs non conscients des avantages apportés par ce dernier

En pratique

- Japon et Chine intègrent IPv6 dans les réseaux nouvellement construits et d'administration
- Europe et Etats Unis, seulement dans les réseaux de recherche et universitaires ou de projets futurs

Les protocoles de couche réseau ARP/RARP – Sommaire

Routage direct et indirect

Objectif d'un routeur suivant les formes de routage

- **Routage indirect** : Déterminer **le routeur** auquel il faut envoyer le datagramme à partir du numéro réseau de l'adresse IP
- **Routage direct** : Machines rattachées sur un même réseau (même numéro de réseau IP)
  E.g. 2 hôtes ou 1 hôte et 1 routeur
  Déterminer **l'adresse physique**du destinataire et encapsulation du datagramme dans une trame

Protocoles ARP et RARP

Permettent de **faire le lien entre les adresses physiques (MAC) et logiques (IP)** d'une même machine

- **ARP (Address Resolution Protocol)** permet de faire correspondre une adresse MAC à une adresse IP donnée
- Et **RARP (Reverse Address Resolution Protocol)** permet l'inverse
  Utilisé lors d'un lancement d'une machine pour demander son IP à un serveur d'adresses

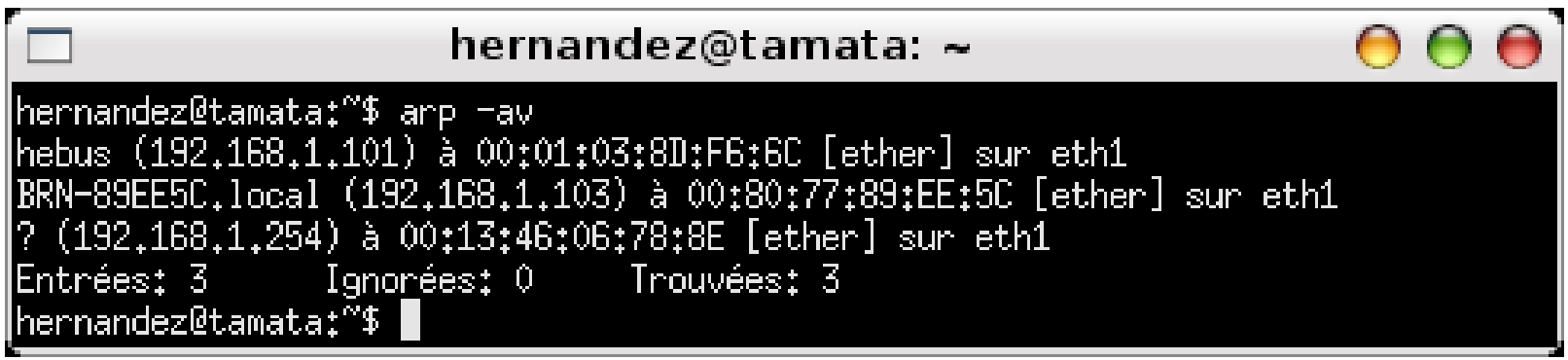
Principe de résolution d'adresses ARP

La résolution d'adresses est effectuée en trois étapes :

1. Le protocole **ARP émet un datagramme particulier qui contient (entre autre) l'adresse IP à convertir, à destination de l'ensemble des stations du réseau**
2. La station **qui se reconnaît retourne un message (réponse ARP) à l'émetteur avec son adresse MAC**
3. L'émetteur dispose alors de l'adresse physique du destinataire et ainsi la couche liaison de données peut émettre les trames directement vers cette adresse physique
   Les **adresses résolues sont placées dans un cache** ce qui évite de déclencher plusieurs requêtes lorsque plusieurs datagramme doivent être envoyés

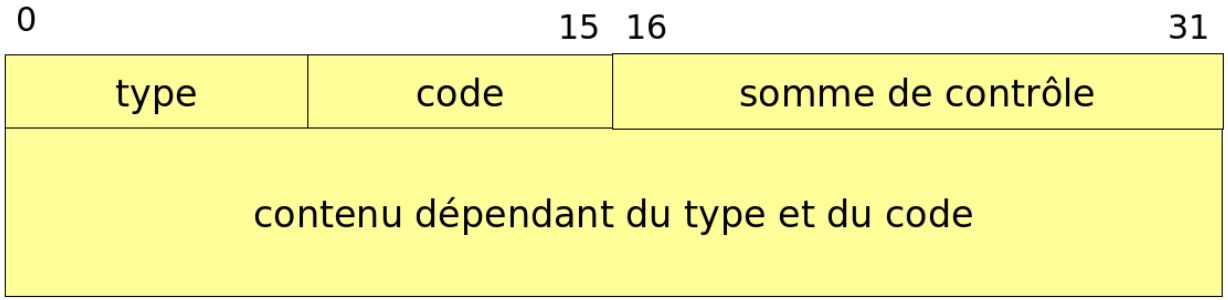
arp

`arp` (sous linux) : consulte, nettoie ou spécifie le cache ARP de la machine locale



Le protocole de couche réseau ICMP – Sommaire

Objectif et Format ICMP



Objectif

ICMP (Internet Control Message Protocol) : Permet de signaler les erreurs de transmission des paquets

Règle : **ne jamais générer un message d'erreur ICMP pour**

- en réponse à un autre message ICMP (exception requêtes ICMP)
- un paquet destiné à une adresse broadcast
- un paquet dont l'expediteur n'a pas une adresse unique (adresse zéro, bouclage, adresse broadcast)
- un fragment autre que le premier

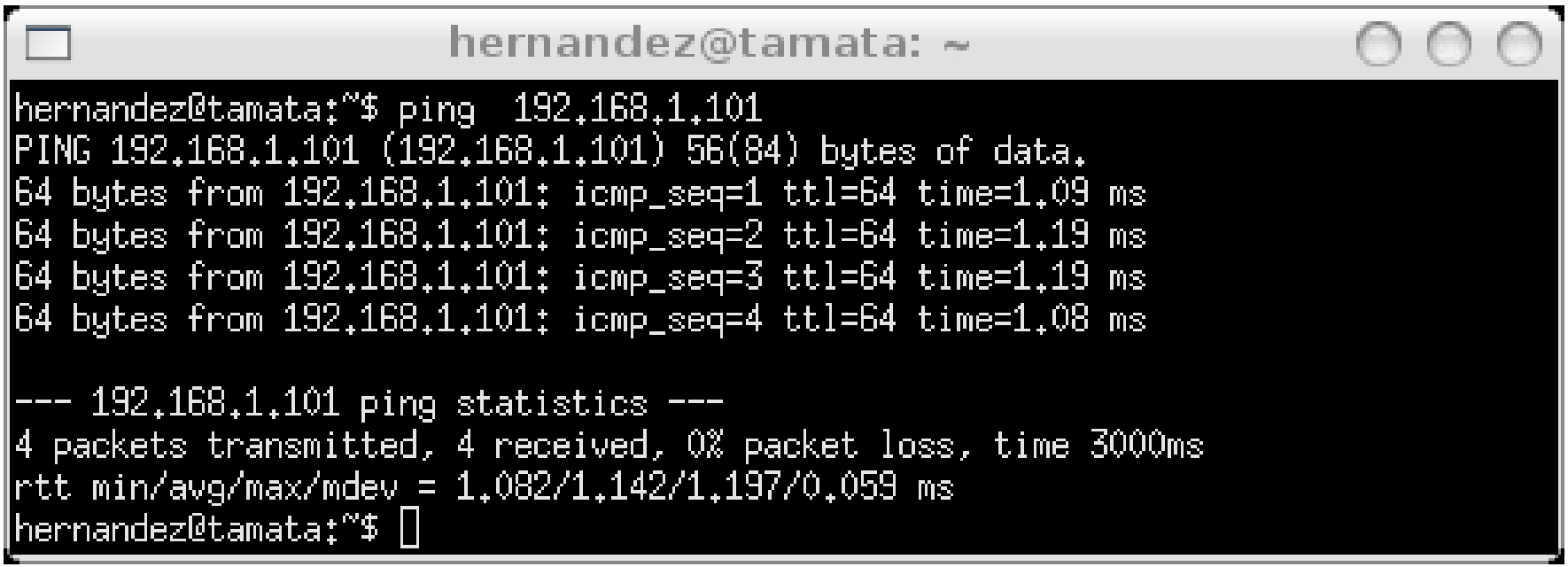
Type et code des paquets ICMP

type	code	description
0	0	réponse echo (ping)
3		destination inaccessible
	0	réseau inaccessible
	1	machine inaccessible
	2	protocole inaccessible
	3	port inaccessible
	4	fragmentation nécessaire
	5	échec de la route source
	6	réseau de destination inconnue
4	0	débit trop élevé
5	0	redirigé
8	0	requête echo (ping)

type	code	description
9	0	avertissement du routeur
10	0	sollicitation du routeur
11		temps dépassé:
	0	TTL vaut 0 pendant le transit
	1	TTL vaut 0 pendant le réassemblage
12		problème de paramètre
	0	mauvaise entête IP
	1	option requise manquante
13	0	requête timestamp
14	0	réponse timestamp
17	0	requête de masque d'adresse
18	0	réponse du masque d'adresse

ping

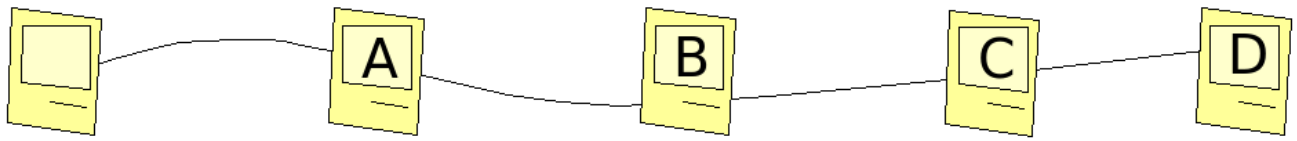
`ping - send ICMP ECHO_REQUEST to network hosts`

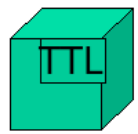


(ici interrompu avec un `CTRL +C`)

Exemple d'utilisation d'ICMP : traceroute

`traceroute IP-de-D` : identification des noeuds intermédiaires jusqu'à D





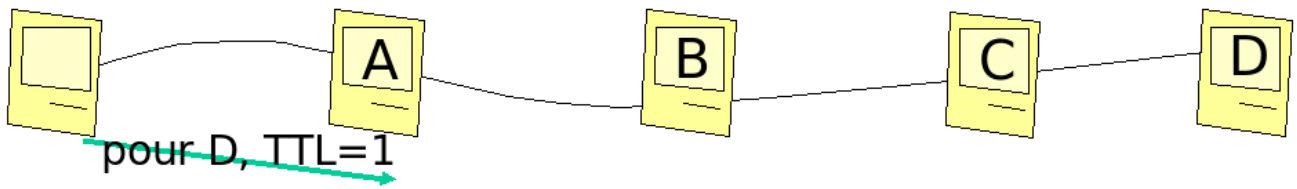
Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

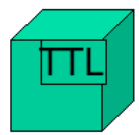
TTL=0 $\rightarrow$ le packet est détruit, un message ICMP en averti l'émetteur

...

Exemple d'utilisation d'ICMP : traceroute

`traceroute IP-de-D` : identification des noeuds intermédiaires jusqu'à D





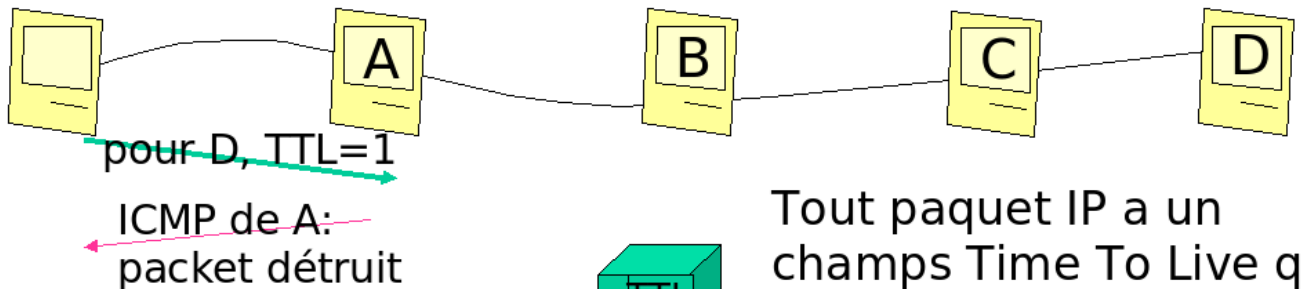
Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 $\rightarrow$ le packet est détruit, un message ICMP en averti l'émetteur

...

Exemple d'utilisation d'ICMP : traceroute

`traceroute IP-de-D` : identification des noeuds intermédiaires jusqu'à D



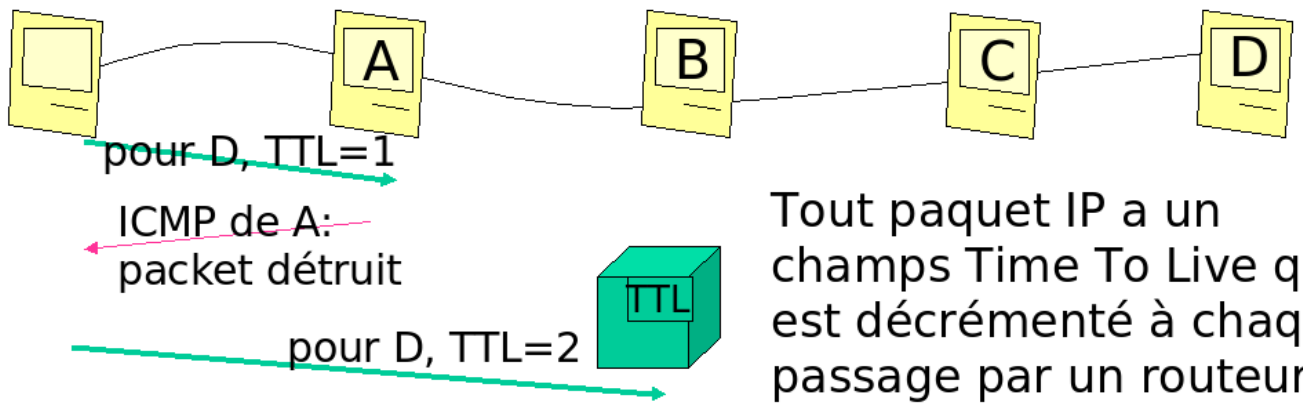
Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 → le packet est détruit, un message ICMP en averti l'émetteur

...

Exemple d'utilisation d'ICMP : traceroute

`traceroute IP-de-D` : identification des noeuds intermédiaires jusqu'à D



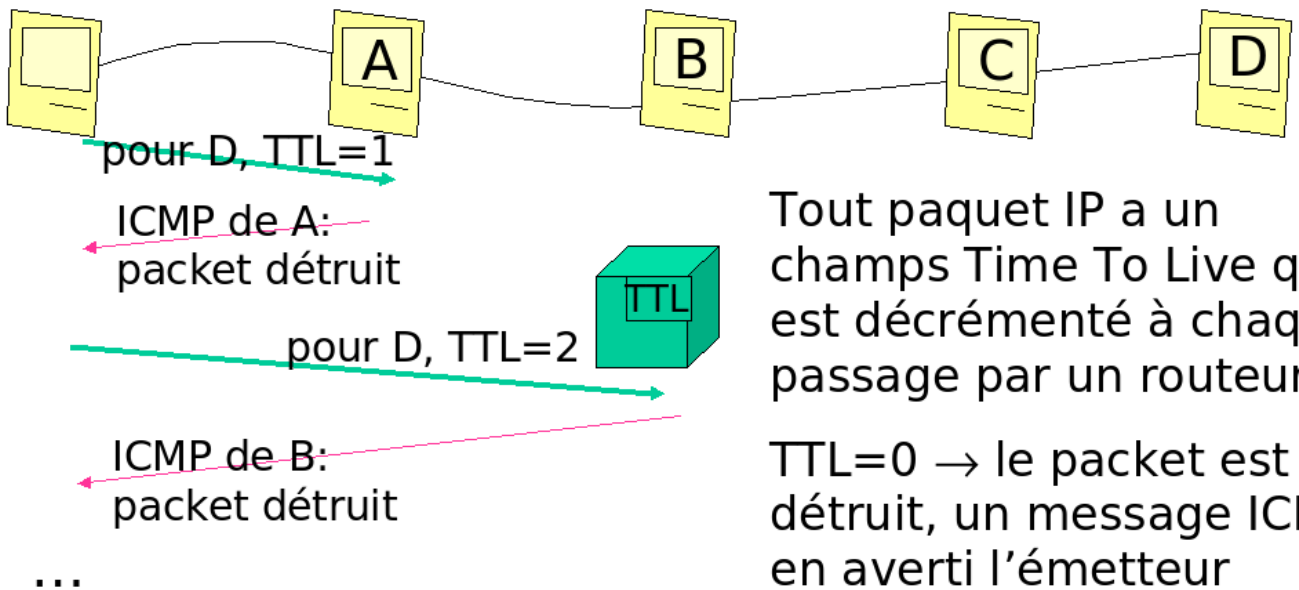
...

Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 → le packet est détruit, un message ICMP en averti l'émetteur

Exemple d'utilisation d'ICMP : traceroute

`traceroute IP-de-D` : identification des noeuds intermédiaires jusqu'à D

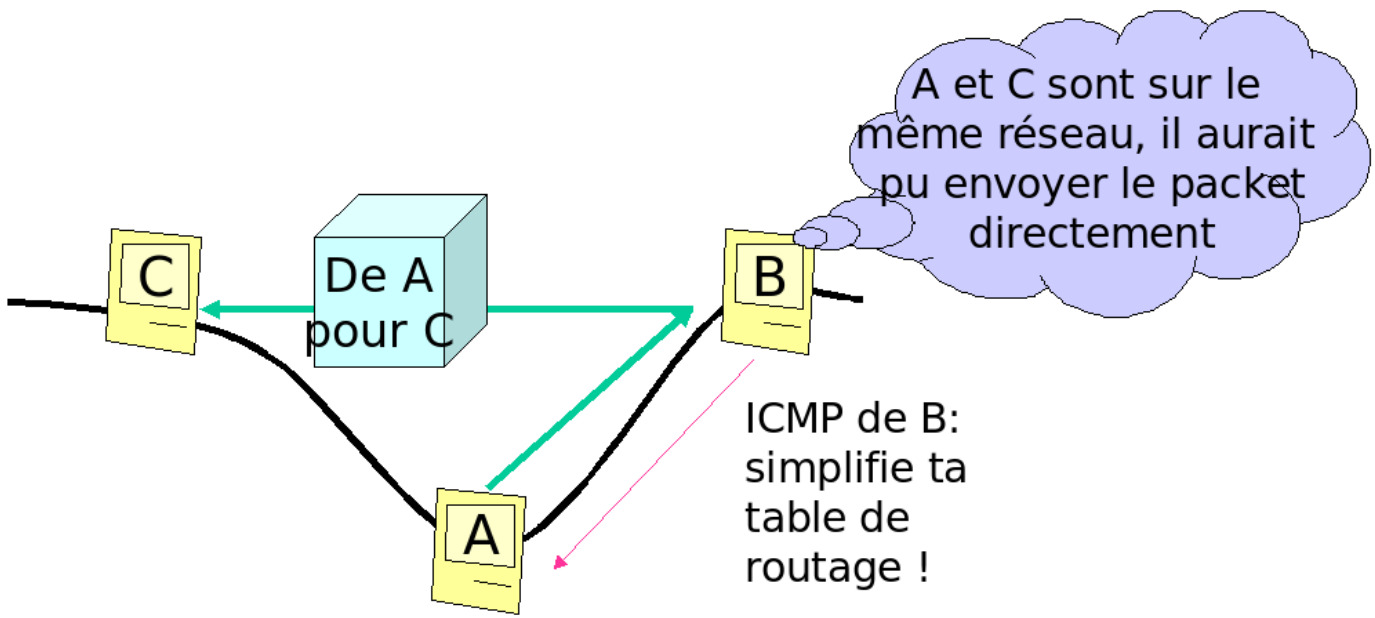


Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 $\rightarrow$ le packet est détruit, un message ICMP en averti l'émetteur

Autre exemple d'utilisation d'ICMP : information de routage

un routeur informe un autre présent sur le même réseau local qu'une meilleure route existe pour joindre un tiers



Rappel : conversion hexadécimal - binaire - décimal

1 octet se code sur 8 bits, 1 hexa se code sur 4 bits

Hex		4				5			
Bin		0	1	0	0	0	1	0	1
↔	Rang des bits	7	6	5	4	3	2	1	0
	2^rang	2^7= 128	2^6= 64	2^5= 32	2^4= 16	2^3= 8	2^2= 4	2^1= 2	2^0= 1
		* 0	* 1	* 0	* 0	* 0	* 1	* 0	* 1
Dec		64 * 1 + 4 * 1 + 1 * 1 = 69							

Quizz de synthèse

- Citer 3 protocoles de la couche réseau
- Quelles différences y a t il entre un adressage physique et un adressage logique ?
- Quels avantages présente l'adressage IPv6 sur l'IPv4 ? Pourquoi l'adressage IPv4 est encore utilisé ?
- Quelles différences y a t il les notions de classe d'adresses et de masque de réseaux ?

Bibliographie

Le présent cours s'appuie sur

Servin ed. 2003 Chapitre 10. L'architecture TCP/IP

Pujolle ed. 2005 Chapitre 3. L'architecture TCP/IP ; Chapitre 7. Le niveau paquet (Adressage et IP) ; Chapitre 17. Les réseaux IP ; Chapitre 18. La gestion et le contrôle dans les réseaux IP

Tanenbaum ed. 1996 Sections 1.4.2-5 The TCP/IP Reference Model, Critique and comparisons with the OSI Model ; 5.5 The network layer in the Internet

Hakin9 2006 (17) Sécurité d'IPv6