

Séance 8 – (Introduction aux) Réseaux

Notes de Cours

VOS ÉLÈVES EN CONVIENDRONT LES PREMIERS, LES RÉSEAUX informatiques sont partout et ils le seront encore davantage dans les prochaines années. Il s'agit d'une avancée technique et scientifique dont les conséquences ont atteint désormais l'ensemble de la société. Internet est l'objet technique le plus gigantesque créé par l'humanité à ce jour. L'objectif de ce mini-module est de vous présenter un aperçu des structures et protocoles réseaux tant du point de vue principes et standardisation (OSI), de ce qui est réellement déployé et de ce qui sera déployé dans un avenir proche (IPv6).

1 Qu'est-ce qu'un Réseau ?

1.a Internet

Internet signifie *interconnexion de réseaux*

L'Internet est ...

- le regroupement d'un ensemble de réseaux très différents : => *protocole commun : IPv4* (IPv6 aussi)
- géré de manière décentralisée (et pragmatique)
- né en 1983 (protocole TCP/IP)
- parvenu au grand public à partir de 1995 : la toile (premier navigateur 1993)

1.b Internet

Il s'agit du plus grand objet technique jamais construit.

Il existe de nombreuses variétés de réseaux rassemblés.

1.c Catégories de Réseaux

De nombreux critères de classification

- Distance** — réseau local (LAN) Ex : 4ème étage
- réseau de communauté urbaine (MAN) Ex : phoceAN

- réseau global (WAN) Ex : RENATER

Topologie — Bus Ex : Ethernet

- Anneau Ex : Token Ring
- Etoile Ex : Ethernet commuté
- Arbre Ex : Ethernet 10baseT
- Maillé Ex : internet-IP, ...

Débit — LAN :

- traditionnel : Ethernet 10, 100, 1000 Mbits/s
- haut débit : ATM 155 ou 622 Mbits/s
- WAN :
- câble sous-marin Europe/Amérique : 32Gbits/s
- liaison louée : 155 Mbits/s
- particulier : faible débit (ex WWW)
- particulier :
- Modem RTC : 56 kbits/s
- ADSL : 2 à 20 Mbits/s (asymétrique)

Mode de Transmissions — filaire : Ethernet

- sans-fil : GSM, WiFi, Bluetooth
- fibre optique : FDDI, AIM, ...

Type de Connexion — sans connexion : datagramme (UDP/IP)

- connecté : (TCP/IP)
- commuté : circuit virtuel permanent (téléphone, ATM)
- avec diffusion : multipoint ou point à point.

Qualité de Service — au mieux : IP

- spécifiée et spécifique : AAL 5, AAL3/4 sur ATM

Nature — dédié : téléphone (filaire ou non)

- banalisé : voix, données, vidéo
- => convergence

1.d Performances

Débit quantité d'information par unité de temps — bits/s : nombre de bits par seconde

- baud : nombre d'information élémentaire par seconde, *un baud peut correspondre à plusieurs bits/s.*

Latence temps entre l'émission et la réception d'un bit *latence = transmission + propagation + attente*

- *transmission = taille/debit*
- *propagation = distance / (k * c), $\frac{2}{3} \leq k \leq 1$*

1.e Nécessité de Protocoles

Un protocole c'est respecter un ensemble de règles

- de communications : langue commune
- de bon fonctionnement : partage de ressources

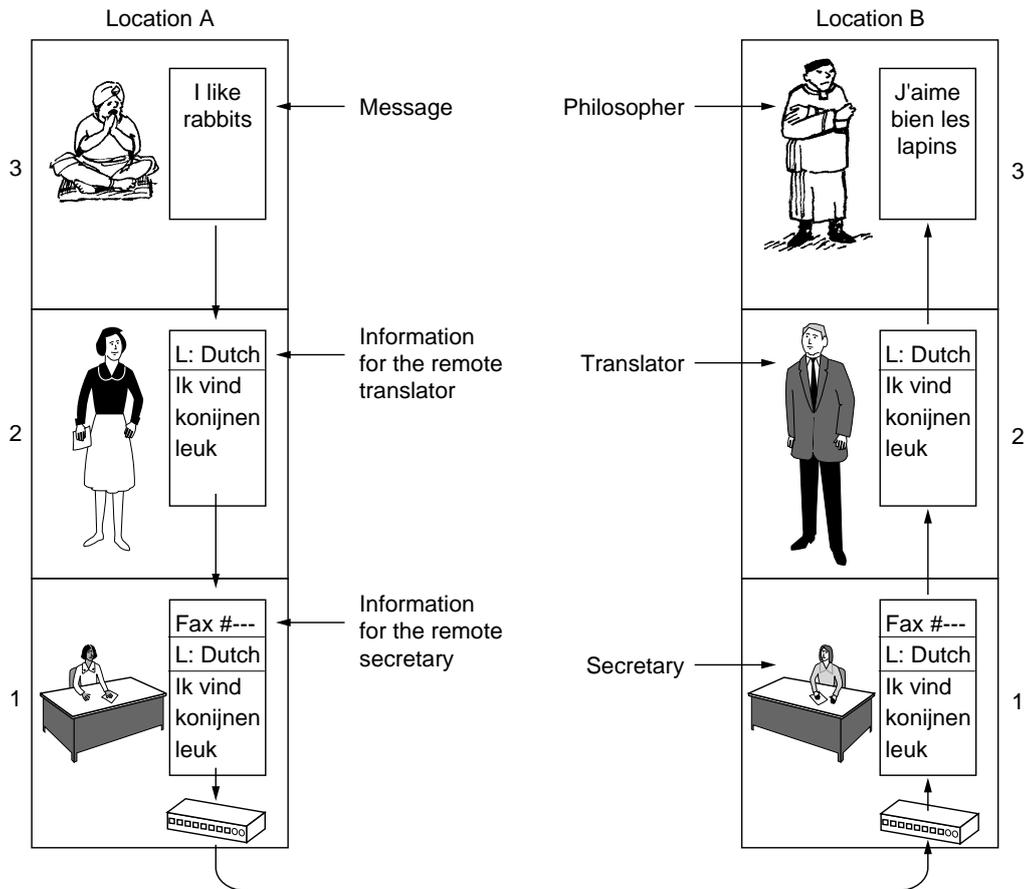
On utilise des protocoles pour :

- utiliser un support physique
- transporter l'information
- utiliser l'information : applications

Les protocoles doivent être *normalisés* mais l'ensemble doit pouvoir être utilisé de la manière la plus décentralisée possible.

1.f Protocoles en Couches

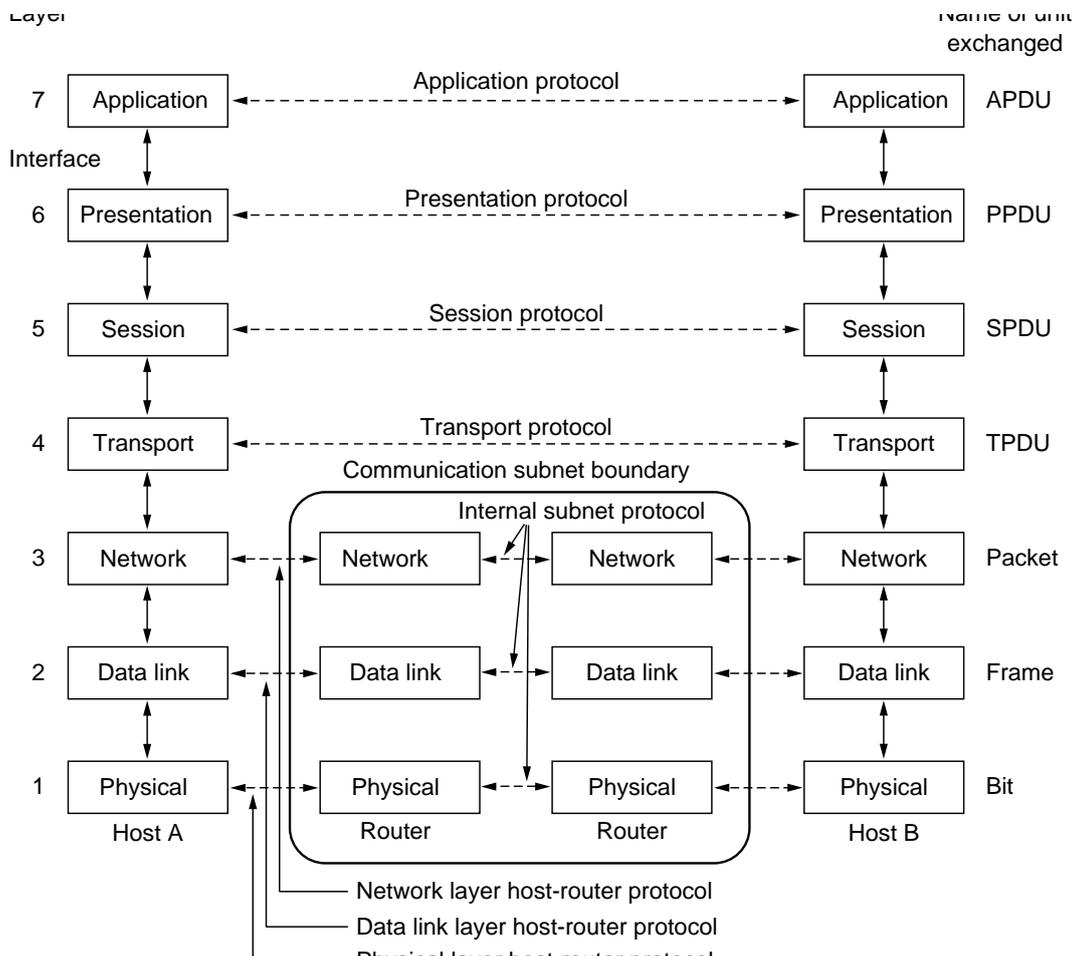
La principale abstraction utilisée est l'architecture en "couches". La *couche supérieure* communique avec la *couche inférieure* par l'intermédiaire d'une *interface*. Cette interface est appelée *API* (*Application Programming Interface*). Elle définit les noms, syntaxes et sémantiques des *méthodes* que la couche supérieure doit manipuler pour pouvoir utiliser la couche inférieure. Ces propriétés (nom, syntaxe et sémantique) sont fixées (au moins un certain temps) et il est possible de modifier les détails de fonctionnement de la couche inférieure sans perturber aucunement le fonctionnement de la couche supérieure.



Traduction d'un format (*anglais*) vers un autre (*français*) en passant par l'intermédiaire d'un troisième (*néerlandais*).

La transmission physique se fait en néerlandais...

1.g Le Modèle OSI : Standard ISO 7498



Physique La couche physique est chargée de la transmission effective des signaux électriques ou optiques entre les interlocuteurs. Son service est généralement limité à l'émission et la réception d'un bit ou d'un train de bits continu.

Cette couche est chargée de la conversion entre bits et signaux électriques ou optiques. Elle est en pratique toujours réalisée par un *circuit électronique spécifique*.

Liaison de Données La couche de liaison de données est la couche de protocole qui transfère des données entre les **nœuds adjacents** d'un réseau. La couche de liaison de données fournit, dans certains cas, les moyens de *détecter et potentiellement corriger les erreurs* qui peuvent survenir au niveau de la couche physique.

Réseau La couche réseau construit une voie de *communication de bout à bout* à partir de voies de communication entre nœuds adjacents. Ses fonctions principales sont donc :

- le routage** détermination d'un chemin permettant de relier les 2 machines distantes ;
- le relayage** retransmission d'un PDU (Protocol Data Unit ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale.
- le contrôle des flux** contrôle de congestion.

Cette couche est donc la seule à être directement concernée par la topologie du réseau. C'est aussi la dernière couche supportée par toutes les machines du réseau pour le transport des données utilisateur : les couches supérieures sont réalisées uniquement dans les machines en bord de réseau.

Transport La couche transport gère les communications de bout en bout entre processus. Cette couche est souvent la plus haute couche où on se préoccupe de la correction des erreurs.

service en mode connecté transfert de messages ou d'octets bruts garantis sans corruption, pertes, réordonnement, duplication.

service en mode non-connecté rien de tout cela (au mieux). A charge aux couches supérieures de gérer ces éventuels problèmes.

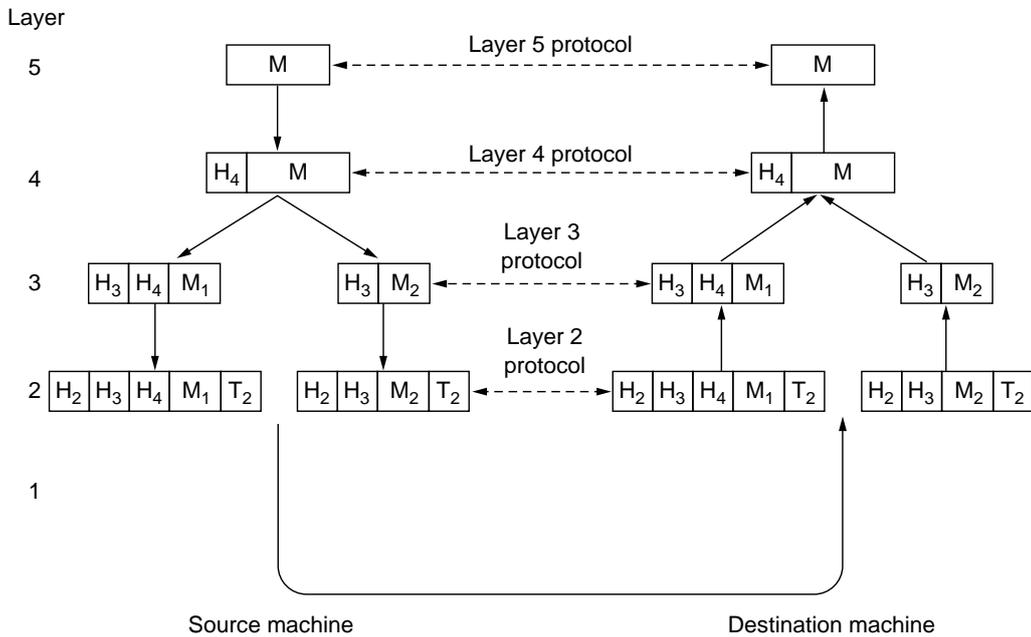
Session Les 2 services originaux de la couche session sont la synchronisation des communications (quel intervenant peut émettre à tel moment) et la gestion des « transactions » (état de session). Un service cependant a été rajouté, c'est un mécanisme de correction des erreurs de traitement par restauration d'un état antérieur connu.

Présentation La couche présentation est chargée du codage des données applicatives. Les couches 1 à 5 transportent des octets bruts sans se préoccuper de leur signification. Mais ce qui doit être transporté en pratique, c'est du texte, des nombres et parfois des structures de données arbitrairement complexes. *Très peu utilisée jusqu'à l'apparition des formats adéquats (XML, Unicode).*

Application La couche application est surtout, du point de vue du modèle OSI, le point d'accès aux services réseaux.

La couche d'application représente des données pour l'utilisateur ainsi que du codage et un contrôle du dialogue : des mécanismes de communication offerts aux applications de l'utilisateur.

1.h Encapsulation des Données



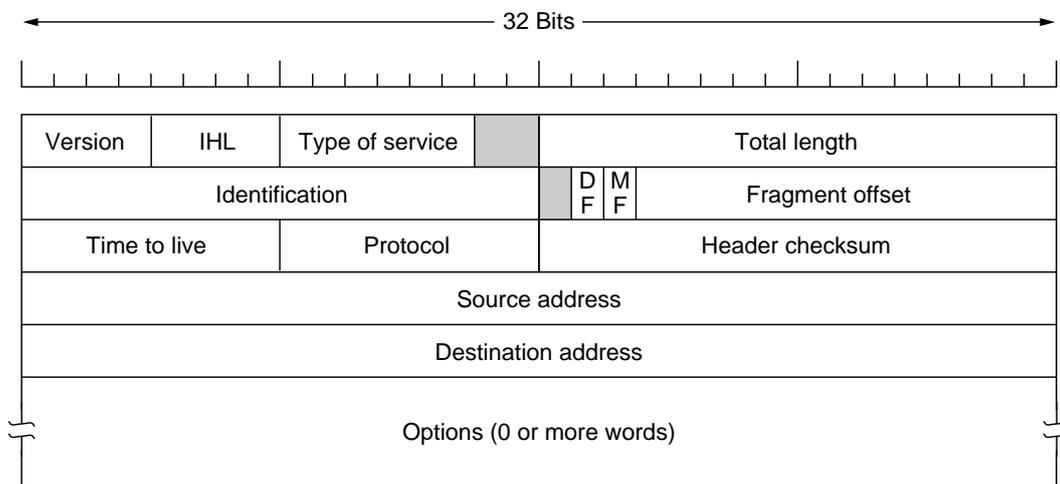
Encapsulation Méthode consistant à inclure les données d'un protocole dans la partie *charge utile* d'un autre protocole

Entête et pied Les données du protocole de la couche supérieure sont *encadrées* par l'entête et le pied de la couche

Entête seul L'entête précède simplement les données. Une indication de taille de la charge utile doit être donnée explicitement dans ce cas.

Remarque Le contenu de la couche supérieure peut être envoyé en plusieurs "blocs" au niveau de la couche inférieure.

1.i Exemple d'encapsulation : entête IPv4



Version (4 bits)

Version d'IP utilisée. Pour IPv4 c'est ... 4.

IHL (Longueur de l'en-tête) (4 bits)

Nombre de mots de 32 bits, soit 4 octets (ou nombre de lignes du schéma). La valeur est comprise entre 5 et 15, car il y a 20 octets minimum et on ne peut dépasser 40 octets d'option (soit en tout, 60 octets).

Type de service (8 bits)

Ce champ permettait à l'origine de définir le ToS (Type of Service - RFC 791). Celui-ci est maintenant défini par la RFC 2474 (Services Différenciés - DSCP). En effet, de nouvelles technologies (comme la VoIP) émergent qui requièrent de la transmission temps-réel, et qui utilisent donc ce champ DSCP.

Longueur totale en octets (16 bits) Nombre total d'octets du datagramme, en-tête IP comprise. Donc, la valeur maximale est (216)-1 octets.

Identification (16 bits)

Numéro permettant d'identifier les fragments d'un même paquet.

Drapeaux (3 bits)

- Premier bit : actuellement inutilisé (doit être 0, voir RFC 3514).
- Deuxième bit : DF (Don't Fragment)
lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté. Si le routeur ne peut acheminer ce paquet (taille du paquet supérieure à la MTU), il est alors rejeté.
- Troisième bit : MF (More Fragments)
quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

Fragment offset (13 bits)

Position du fragment par rapport au paquet de départ, en nombre de mots de 8 octets.

Durée de vie ou TTL Time To Live (8 bits)

Initialisé par l'émetteur, ce champ est décrémenté d'une unité généralement à chaque *saut* de routeur. Quand TTL = 0, le paquet est abandonné et un message ICMP est envoyé à l'émetteur pour information.

Protocole (8 bits)

Numéro du protocole au-dessus de la couche réseau : TCP = 6, UDP = 17, ICMP = 1.

Somme de contrôle de l'en-tête ou Checksum (16 bits)

Complément à un de la somme complémentée à un de tout le contenu de l'en-tête afin de détecter les erreurs de transfert. *Si la somme de contrôle est invalide, le paquet est abandonné sans message d'erreur.*

Adresse source (32 bits)

Adresse IP de l'émetteur sur 32 bits.

Adresse destination (32 bits)

Adresse IP du récepteur 32 bits.

Options (0 à 40 octets par mots de 4 octets)

Facultatif.

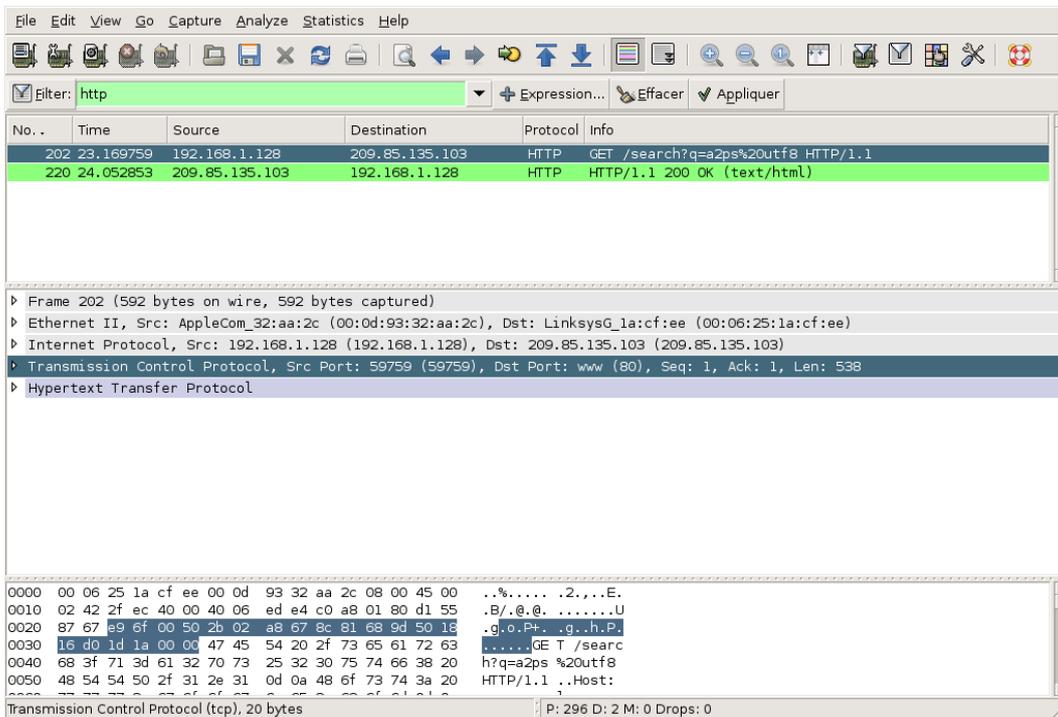
Bourrage de taille variable comprise entre 0 et 7 bits.

Il permet de combler le champ option afin d'obtenir un en-tête IP multiple de 32 bits. La valeur des bits de bourrage est 0.

Note finale codage des entiers

Depuis la RFC 1700, la plupart des protocoles réseaux codent les entiers en gros-boutiste. C'est bien le cas ici.

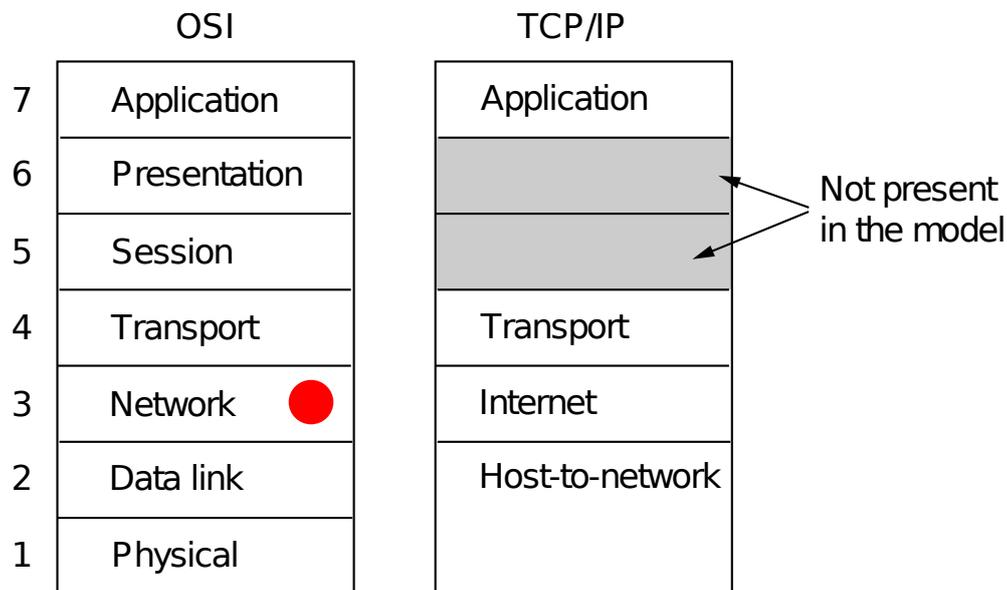
1.j Analyse du Trafic Réseau



Le logiciel wireshark que nous utiliserons en TP permet très simplement de visualiser les couches.

1.k La Réalité

TCP/IP, ATM, ... ne respectent pas le modèle OSI mais ont été adoptés *pragmatiquement*.



2 Les Espaces de Noms en Réseaux

2.a Espace de Noms

Déf. ensemble fini d'éléments auxquels est associé une représentation machine

On les appelle en général adresse dans le contexte des réseaux

- adresse MAC (couche 2)
- adresse IPv4 (couche 3)
- adresse IPv6 (couche 3)
- numéro de port (couche 4)
- adresse DNS
- URL

Il peut exister une correspondance entre espace de noms, par *résolution*.

2.b Adresses Ethernet/MAC

- Adresses uniques sur 48 bits (attribuées à la fabrication de la carte réseau)
- 3 types d'adresse reconnue par le coupleur
 - adresse physique d'un coupleur EUI-48
 - 24 bits fabricant (OUI attribué par l'IEEE)
 - 24 bits n° de série
 - diffusion générale (broadcast)
 - FF:FF:FF:FF:FF:FF
 - diffusion multidestinataires (multicast) (bit de point faible du premier octet à 1)
 - 01:80:C2:00:00:00

2.c Nommage : Adresses Internet

Ce sont des adresses **mondiales** *logiques*

- sur 4 octets en IPv4
- sur 16 octets en IPv6

Notation pointée en IPv4 :

- chaque octet est donné en décimal,
- l'octet de poids fort est donné le premier,
- chaque octet est séparé par un "."
- **indirection** possible (DNS)

Ex : le serveur de l'environnement numérique de travail (`ent.univ-amu.fr`) a pour adresse IPv4 `139.124.244.83`.

2.d Attribution des Adresses Internet

Adresse = identifiant **unique**, en nombre limité (en IPv4)

- Enjeu de pouvoir
- Gestion centralisée pour l'unicité, déléguée pour la pratique
- Les adresses (numéro IP) sont attribués par l'IANA (composante de l'ICANN - Internet Corporation for Assigned Names and Numbers)

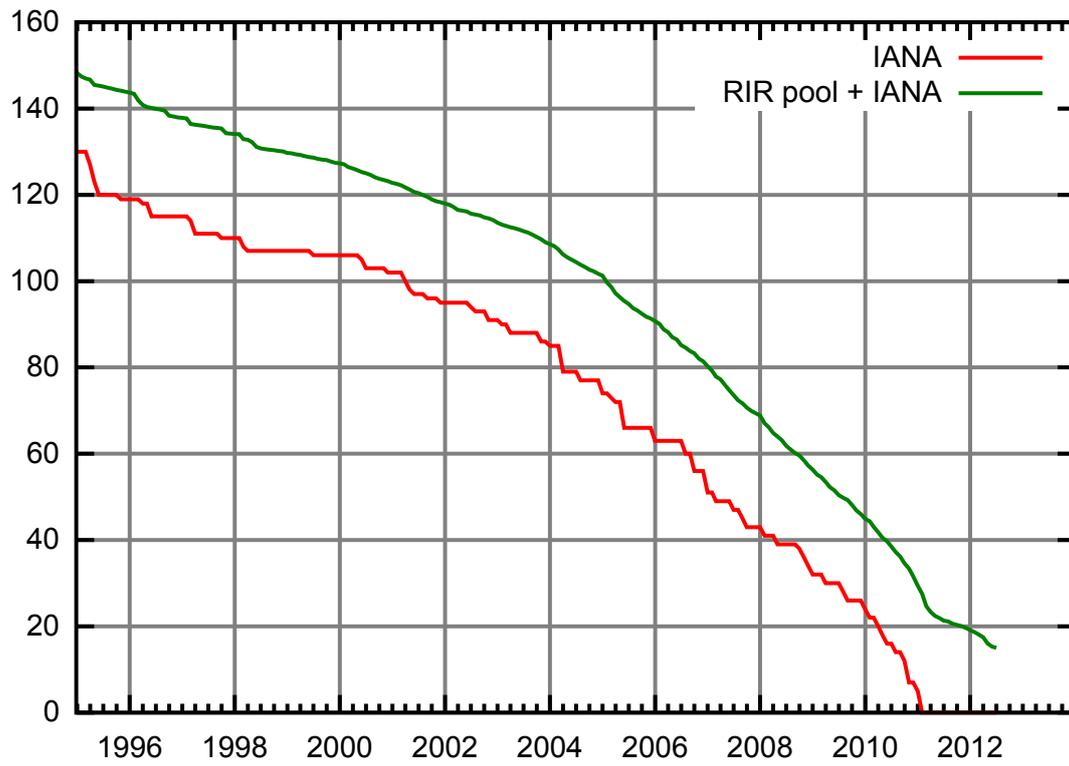
La gestion pratique est déléguée à divers organismes et sociétés privées (Ex : VeriSign, ...)

Par exemple, leurs fonctions sont déléguées au niveau continental

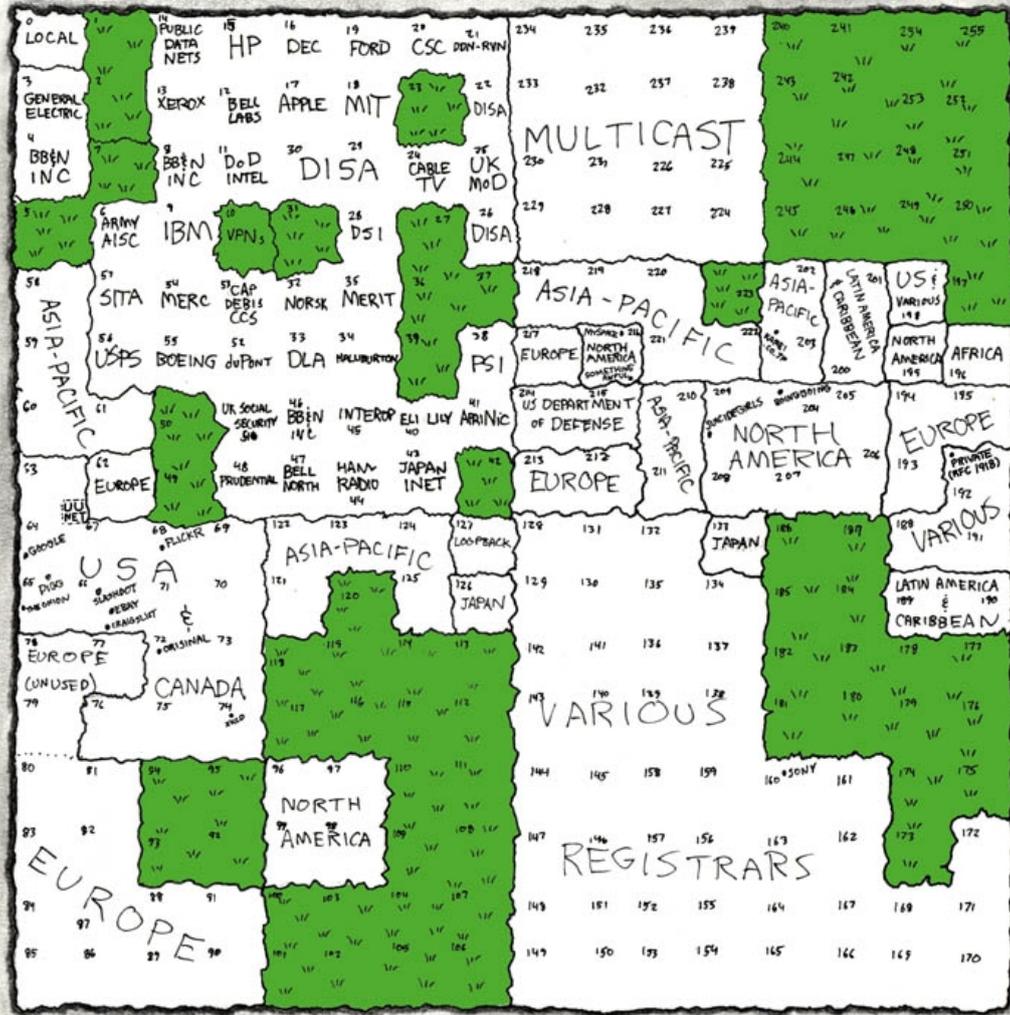
- RIPE (Réseaux IP Européens)
 puis déléguées au niveau national
- à des répertoires Internet Locaux Ex : AFNIC puis déléguées
- à un gestionnaire de réseaux Ex : RENATER, qui délègue au niveau local
- à un administrateur Ex : DOSI de l'Université qui délègue au niveau du campus
- à un administrateur Ex : DOSICALU pour Luminy

2.e Epuisement des adresses IPv4

~ 4 milliards initialement disponibles mais **pénurie d'adresse** car la **demande est très importante** (et il y a eu un peu de gaspillage notamment pour les réseaux "historiques" ...)

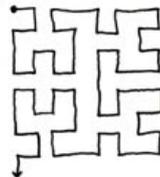


2.f Répartition



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

0	1	14	15	16	19 →
3	2	13	12	17	18
4	7	8	11		
5	6	9	10		



 = UNALLOCATED BLOCK

Une Vision Fractale d'Internet (xkcd.com)

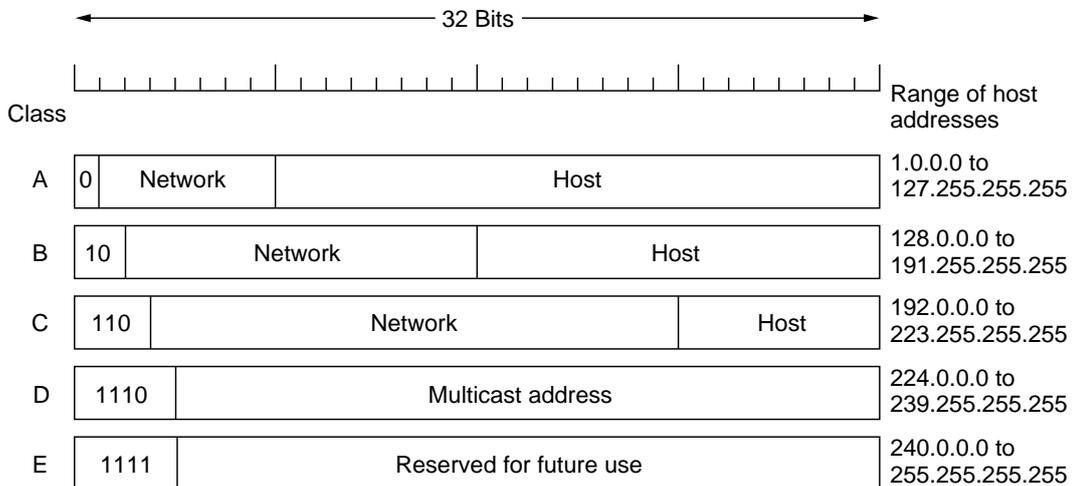
2.g Classes d'Adresses

Une *classe d'adresses* est un **ensemble** d'adresses. Ces ensembles sont *structurés* pour faciliter l'organisation.

=> Cinq classes d'adresses en IP v4 : A, B, C, D ou E Déterminées à partir des 4 bits de poids fort du premier octet

- 0xxx : adresse de classe A
- 10xx : adresse de classe B
- 110x : adresse de classe C
- 1110 : adresse de classe D
- 1111 : adresse de classe E

2.h Adresses IP et Classes d'Adresse



2.i Des Classes d'Adresses ...

On "divise" chaque adresse

- début : partie réseau
- fin : machine de ce réseau

=>

- adresse de réseau
- adresse de machine

La classe d'un réseau indique

- Classe (A) 1 octet pour le réseau et 3 pour la machine
- Classe (B) 2 octets pour le réseau et 2 pour la machine
- Classe (C) 3 octets pour le réseau et 1 pour la machine

en fonction de sa classe, une adresse de réseau peut contenir plus ou moins d'adresses de machines

- ~ 16 millions en classe A
- ~ 65000 en classe B
- 254 (= 256 - 2) en classe C

2.j Exemple de Classes d'Adresses

- Pour représenter l'adresse du réseau, tous les bits correspondant à l'adresse de la machine sont mis à zéro (convention)
- Exemple : l'adresse 192.55.6.2 est de classe C
- 11000000.00110101.00000110.00000010
 - L'adresse du réseau est donc 192.55.6.0
 - L'adresse de la machine dans ce réseau est 2
- Les adresses de classe D sont des adresses de groupe (multicast) : de 224.0.0.0 à 239.255.255.255
- Les adresses de classe E sont réservées

2.k ... Aux Masques de Réseaux

- Le découpage par classes est **trop rigide**
- La notion de masque de réseau permet de « couper » les deux parties n'importe où (ailleurs qu'aux octets « ronds »)
 - Il s'agit d'une adresse composée d'un nombre de bits à 1 au début, et tout le reste à 0
 - Remplace et affine la notion de classe (notation *CIDR*)
 - CIDR signifie *Classless Inter Domain Routing*

2.1 Exemple d'ensemble d'adresses (avec masque CIDR)

On note 10.65.67.12 / 255.224.0.0 ou encore 10.65.67.12 / 11

Adresse	00001010.01000001.01000011.00001100	10.65.67.12
Masque	11111111.11100000.00000000.00000000	255.224.0.0
Réseau	00001010.01000000.00000000.00000000	10.64.0.0
Machine	00000000.00000001.01000011.00001100	0.1.67.12

2.m Composition de Réseaux

- On peut ainsi :
- découper un réseau en sous-réseau
 - regrouper des sous-réseaux
 - => utilisé pour hiérarchiser et "ordonner" la topologie du réseau pour le routage, réduire la taille des tables de routage.

2.n Adresses IP Réservées

- 127/8 : cet hôte (boucle locale)
- `reseauA.255.255.255` : diffusion sur réseau de classe A
- `reseauB.255.255` : diffusion sur réseau de classe B
- `reseauC.255` : diffusion sur réseau de classe C
- 10/8, 172.16/12, 192.168/16 : adresses privées (=> *non routées sur internet*)
- 169.254/16 : adresses de configuration automatique (=> *non routées*)



Une *adresse* peut donc désigner à la fois une machine ou un **ensemble** de machines.

2.o Pour Résumer : Adresse IPv4

- espace de noms mondial sur 4 octets
- les stations sont regroupées en sous-réseaux de machines ayant le *même préfixe* pour des raisons d'efficacité
- la taille du préfixe (le masque CIDR) est arbitraire et propre au sous-réseau.

2.p Address Resolution Protocol (ARP)

Chaque hôte possède une table ARP

- adresse MAC \longleftrightarrow adresse IP
- enregistrement de durée de vie courte (< 20 min)
- enregistrement manuel Ex : `arp -s`
- enregistrement par requête ARP :
 - Qui possède cette adresse IP? **en diffusion**
 - Seule la machine concernée répond
 - Les deux machines mettent leur table à jour

2.q Numéro de port

- entier sur 16 bits, représenté en décimal en général
- permet d'étendre l'espace de noms pour les applications :
adresse IP + n° de port

2.r Adressage IPv6

Beaucoup plus d'adresse disponibles : 2^{128}
=> 667 millions de milliards d'adresses IP disponibles
par mm^2 de la surface de la Terre;

2.s Notation IPv6

Plus de *notation pointée* mais uniquement de l'*hexadécimal*

— exemple

2001:0db8:0000:85a3:0000:0000:ac1f:8001

— possibilité de supprimer les 0 non significatifs par groupes de 1 à 3

2001:db8:0:85a3:0:0:ac1f:8001

— voire par blocs entiers de 4

2001:db8:0:85a3::ac1f:8001

2.t Particularités

— Cohabitation avec les ports de TCP/UDP

— `http://[2002:400:2A41:378::34A2:36]:8080`

2.u Notation CIDR

On conserve la notation CIDR :

— adresse/taille

<=> préfixe de l'ensemble d'adresses considérées

— exemple `2001:db8:1f89::/48`

2.v Type d'adresses IPv6

Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques
fe80::/10	Adresses liens locaux
ff00::/8	Adresses multicast

2.w Adresses Réservées

— :: adresse non spécifiée (début de configuration...)

— ::1/128 adresse *localhost* (comme 127.0.0.1 en IPv4)

— adresses permanentes 2001::/16

— adresses réservables par blocs /12 à /23 depuis 1999.

— 2001::/32 est utilisé pour le protocole de tunnel Teredo

— 2002::/16 est utilisé par 6to4

3 DNS

3.a Les Noms ICANN

- Composés d'étiquettes (caract. alphanumériques ascii, pas d'espace) séparé par des .
 - au plus 63 caractères par étiquette
 - au plus 255 caractères au total
 - la casse ne compte pas
- Organisés hiérarchiquement *de la droite vers la gauche*
 - `lif.univ-mrs.fr` est un sous-domaine de `univ-mrs.fr`, qui est un sous-domaine de `fr`
 - pour *résoudre* un nom :
 - **pas de diffusion!**
 - appel au serveur DNS local
 - le DNS local fait appel au DNS du domaine distant
 - ou bien, faire appel aux *serveurs racines* : `a.root-server.net`, ...

`ent.univ-mrs.fr` a pour IP `147.94.67.3`

`ent.univ-mrs.fr` IN A "147.94.67.3"

3.b Domaine de plus Haut Niveau (TLD)

Ces domaines ont des objectifs et des politiques d'attribution différentes

- `.net` : infrastructure du réseau
- `.com` : services commerciaux (+ législation de la marque déposée)
- `.org` : organisations (au sens très large)
- depuis 2000 : `.aero`, `.biz`, `.coop`, `.info`, `.museum`, `.name`, et `.pro`
- ccTLD : `.fr`, hôtes résidant en France (géré par l'AFNIC)
- depuis 2011 : généralisation des gTLD (le `.bidule` est à 185000\$, plus 25000\$ annuels)

3.c Système DNS

Le système DNS est une brique essentielle d'Internet
protocole DNS pour la résolution

- nom -> adresse IPv4/IPv6
- adresse IPv4/IPv6 -> nom

3.d URLs et URIs

- URI : "Uniform Resource Identifier", possède neuf champs. Exemple :
 - `mailto:egoddard@cmi.univ-mrs.fr`
 - `urn:isbn:096139210x`
 - `ftp://egoddard@mimosa.univ-mrs.fr/`

- URL : “Uniform Ressource Locator”, pour le World Wide Web, de la forme
protocole://serveur.domaine[:port]/chemin
peut être relatif (dépendant de l’URL courante).

Remarque : `http://www.cmi/~egodard/ens/reseaux/index.html#tp`
est une URI pas une URL...

3.e URLs et Espace de Noms

Les URLs sont basés sur plusieurs espaces de noms

- Ports :
 - `http : 80`, en clair
 - `https : 443`, protégé via SSL/TLS
- Nom de domaine (DNS)
- Chemin local (serveur)