ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

Architectures matérielles et logicielles des réseaux

S. Genaud

illustrations modèles réseaux par Philippe Latu

illustrations routage internet par Julien Gossa

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

Partie 1 : architecture

Modèle OSI, modèle TCP/IP, et lien entre les deux, Rôle des différentes couches, Format des messages IP, TCP, UDP

Modèle OSI

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Norme ISO 7498 (dernière rev 1994)
- Cadre général pour créer des normes cohérentes.
- Le modèle ne définit ni service ni protocole.
- Modèle à 7 couches:
  - 4 couches inférieures orientées communication (typiquement fournies par un OS)
  - les 3 couches supérieures orientées applications (fournies par des bibliothèques ou des programmes)
- Les couches sont isolées: une couche ne peut communiquer qu'avec ses couches du dessus et du dessous

Modèle OSI

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

① couche **physique** transmission effective des signaux. Typiquement limité à l'émission/réception de bits.

② couche **liaison de données** : gère les communications entre 2 machines adjacentes, directement reliées entre elles par un support physique.

③ couche **réseau** gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.

④ couche **transport** : gère les communications de bout en bout (ex. d'un programme à l'autre)

⑤ couche **session** : gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.

⑥ couche **présentation** : codage des données applicatives, (conversion entre données manipulées au niveau applicatif et octets transmis).

⑦ couche **application** est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

Couche liaison de données (Data Link Layer)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- structure les flots de bits transportés par la couche physique en **trames**.
- a la charge de faire du **contrôle d'erreur** (dans Ethernet, utilisation du FCS).
- éventuellement, du **contrôle de flux** (empêcher par exemple qu'une station émette en continu)

- *représentant connu : Ethernet*

Couche réseau (Network Layer)

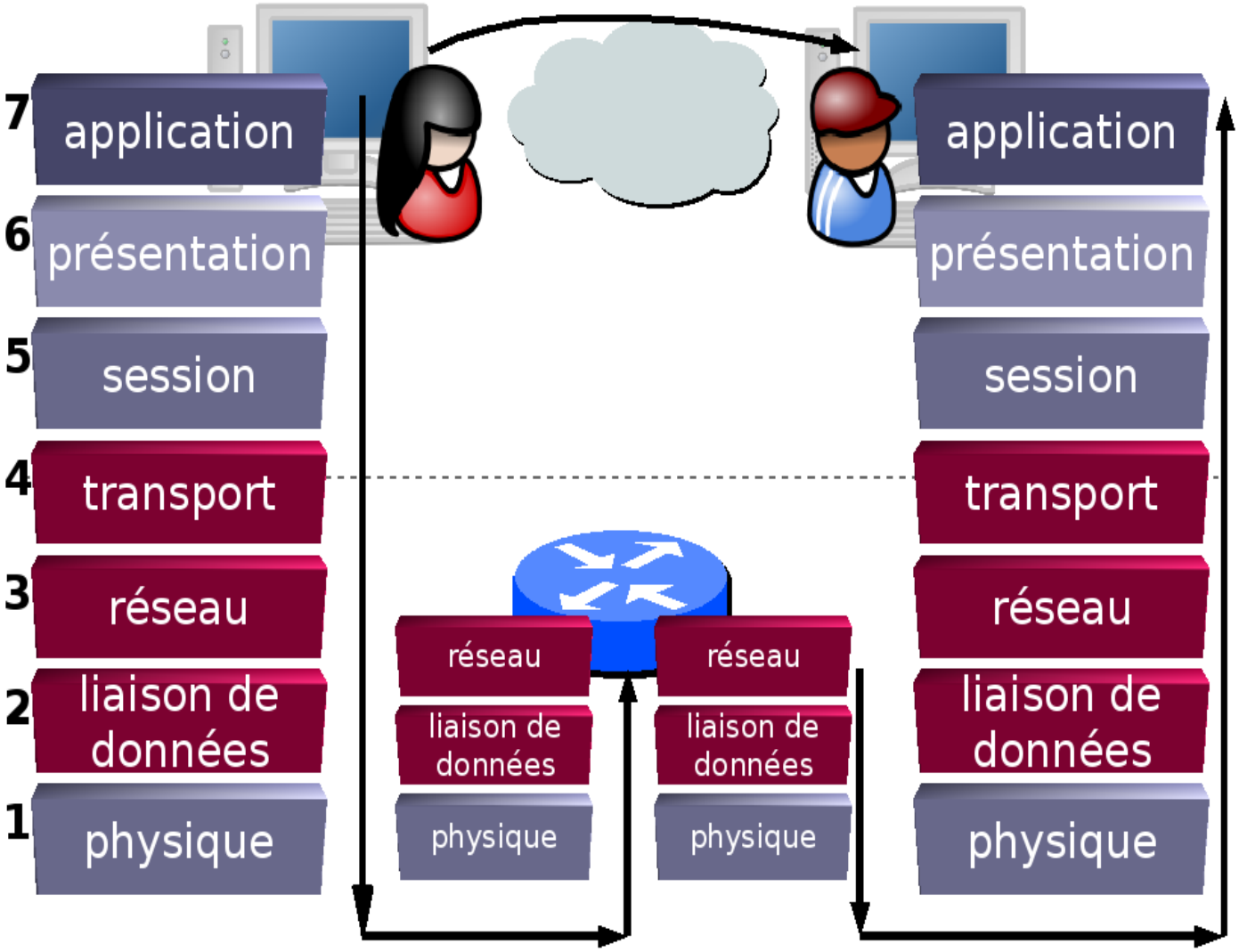
ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- L'information est structurée en **paquets**
- Gère l'**acheminement** de l'émetteur au récepteur.
  - nécessite de faire du routage
  - gérer interconnexion entre réseaux hétérogènes => changement format adresse, redimensionnement paquets, ...
- Gère qualité de service par des messages de régulation

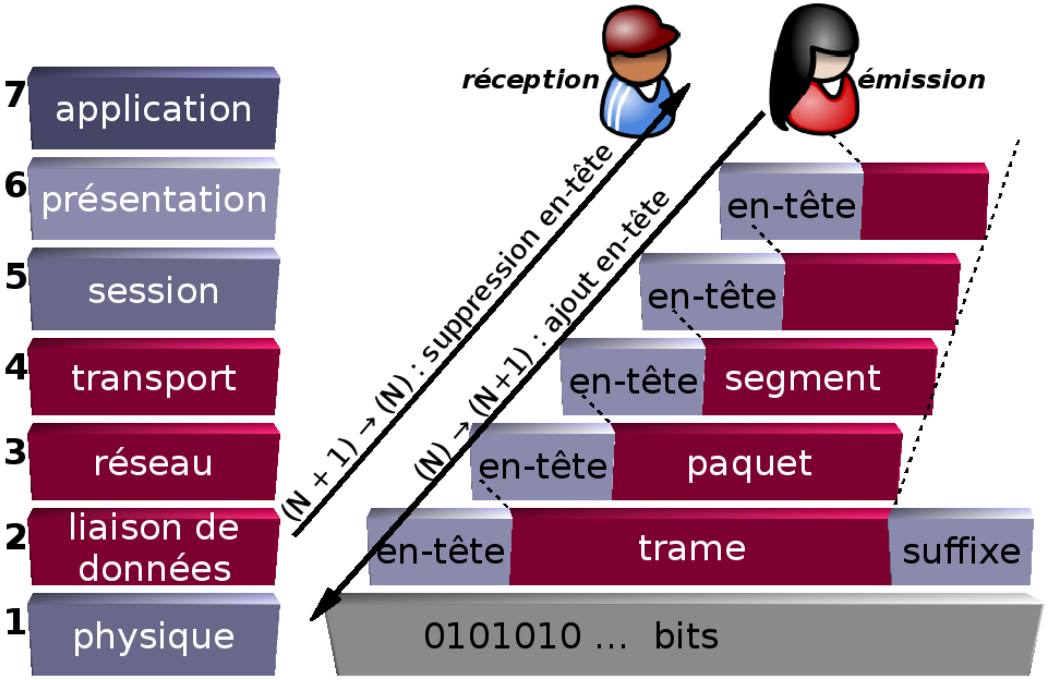
- *représentant connu : IP*

Modèle OSI

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

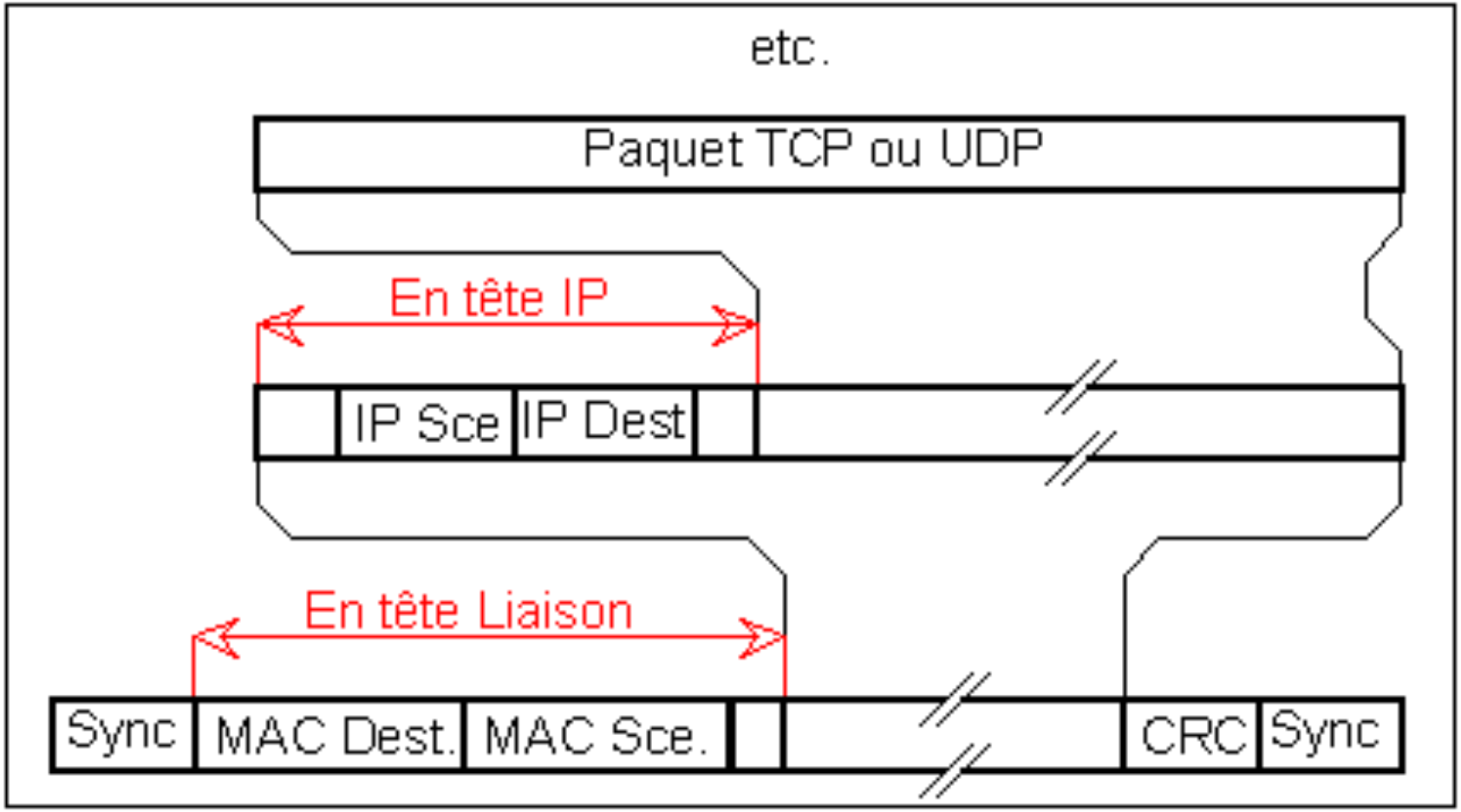


Encapsulation



- Analogie lettre-enveloppe-sac postal-..
- Fragmentation : longueur trames limitée (dépend du matériel) : MTU
  - ex MTU en octets: Ethernet 1500, IEEE 802.3 1492, Token Ring 4440--17940, X.25 1007
  - Il faut donc découper les messages de niveau supérieur pour les faire entrer dans des trames du réseau local considéré.

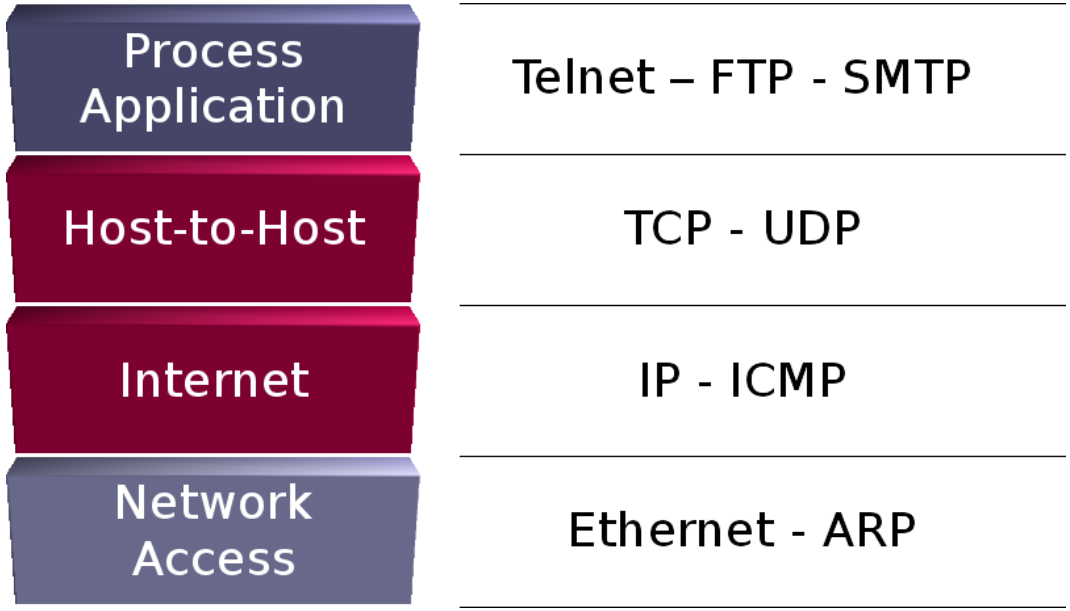
Encapsulation



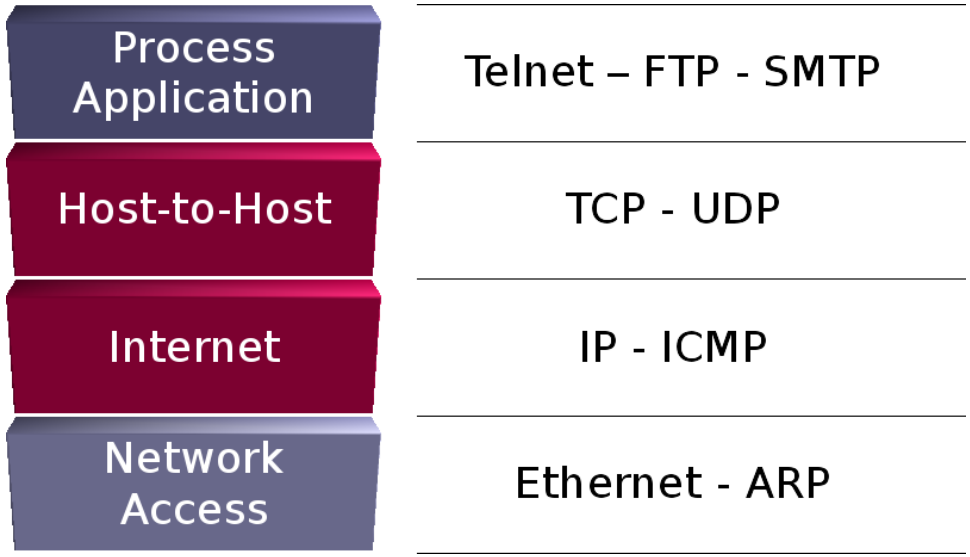
TCP/IP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Créé avant le modèle OSI (ARPANET,1974)
- Objectif: relier des réseaux différents



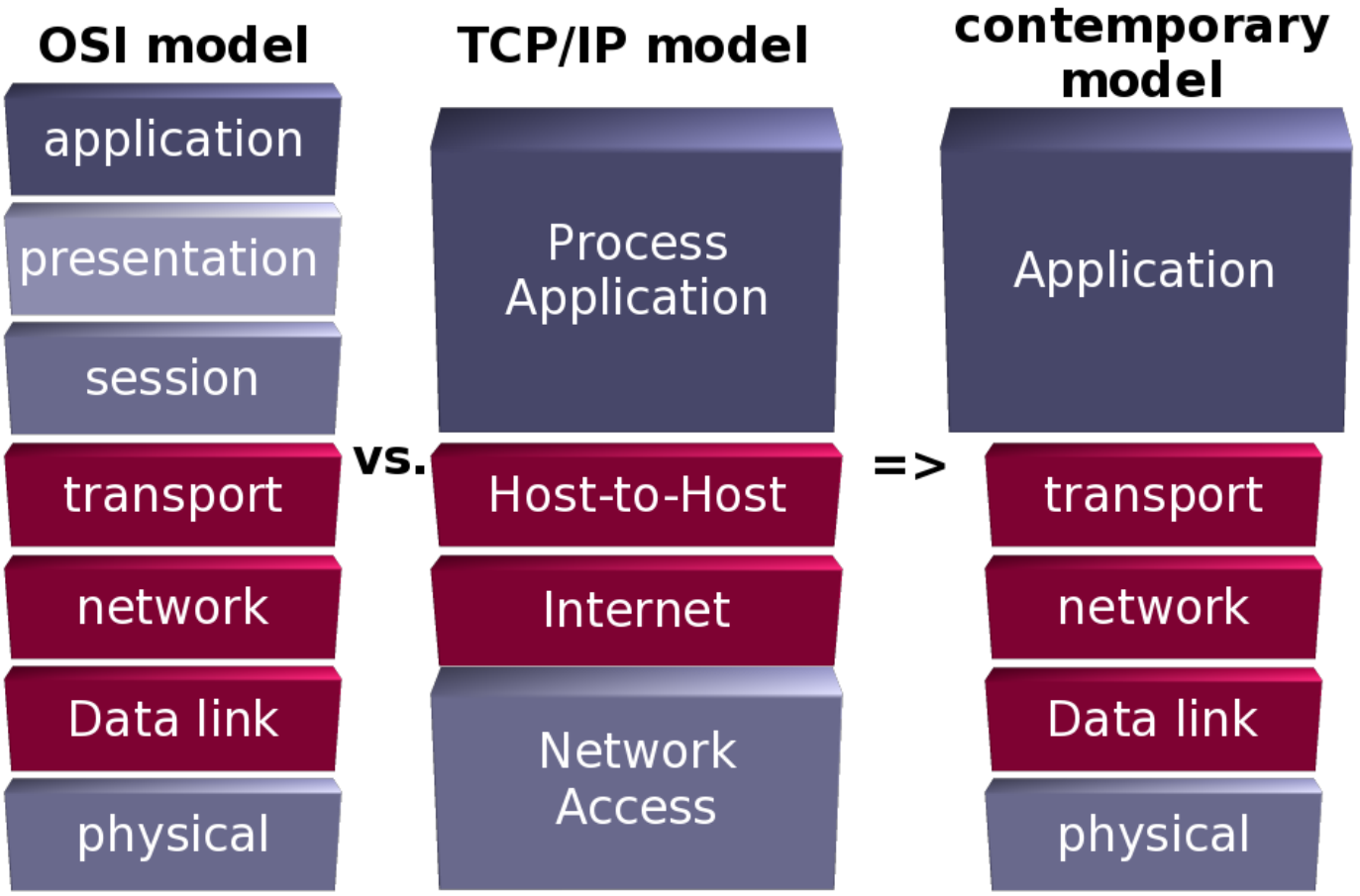
TCP/IP



- ***Network Access*** transmet les données sur le média physique. En fonction du type de réseau, différents protocoles peuvent être utilisés.
- ***Internet*** transmet de source à destination, en gérant l'hétérogénéité des réseaux. Protocoles de routages.
- ***Host-to-Host*** gestion de connexion, contrôle de flux, retransmission des données perdues.
- ***Process/Application*** protocoles de niveau utilisateur

OSI vs TCP/IP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise



IP (Internet Protocol)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- IP est le protocole utilisé par internet permettant un service d'**adressage unique**.
- Protocole de niveau 3 OSI (couche réseau) : reçoit segments de la couche 4 transport (TCP) et les transmet à la couche 2 (e.g. Ethernet).

- protocole non-orienté connexion : les paquets peuvent emprunter des routes différentes.
- Fiabilité : pas de garantie
  - de corruption des données
  - de séquencement des paquets (ordre d'arrivée)
  - de perte de paquets (pas de mécanisme de ré-émission)

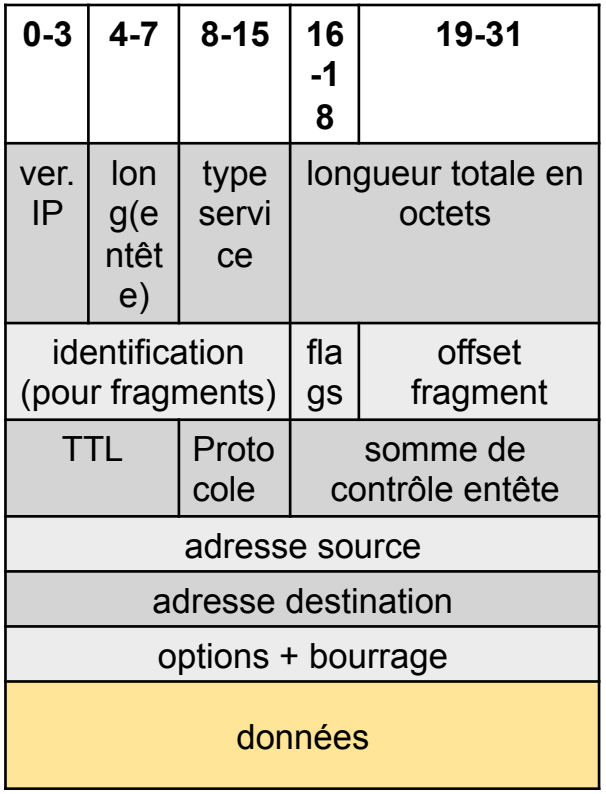
Paquet IP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

<table>
<tr><th>0-3</th><th>4-7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>ver. IP</td><td>long(entête)</td><td>type service</td><td colspan="2">longueur totale en octets</td></tr>
<tr><td colspan="3">identification (pour fragments)</td><td>flags</td><td>offset fragment</td></tr>
<tr><td colspan="2">TTL</td><td>Protocole</td><td colspan="2">somme de contrôle entête</td></tr>
<tr><td colspan="5">adresse source</td></tr>
<tr><td colspan="5">adresse destination</td></tr>
<tr><td colspan="5">options + bourrage</td></tr>
<tr><td colspan="5">données</td></tr>
</table>

Paquet IP

- version : ici 4
- long(entête) : nb lignes
- type service : priorité (rare)
- longueur, entête comprise (max 2^{16} = 65536 octets)
- identification : pour identifier fragments d'un même paquet
- flags: bit 17 à 1 : ne pas fragmenter, bit 18 à 1: fragmenté (fragments à suivre)
- offset: position du fragment rel. au paquet départ (en mot de 8 octets)
- protocole : numéro du protocole au-dessus de la couche réseau : TCP = 6, UDP = 17, ICMP = 1.



Paquet IP : fragmentation

0-3	4-7	8-15	16-18	19-31
ver. IP	Long. entête	type service	longueur totale en octets	
identification (pour fragments)			flags	offset fragment
TTL		Protocole	somme de contrôle entête	
adresse source				
adresse destination				
options + bourrage				
données				

Exemple :
M=3500, MTU=1500,
entête=20

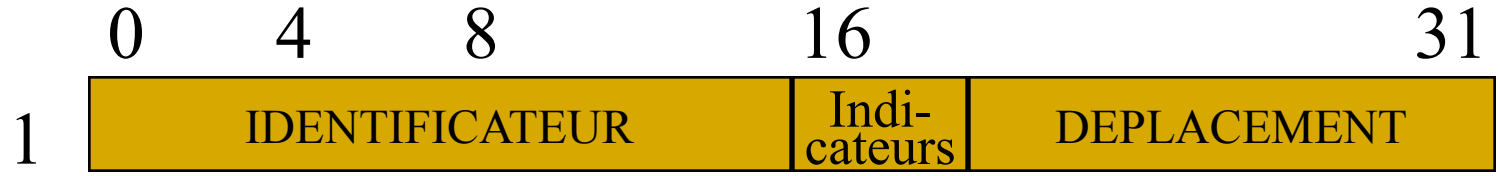
MF / offset / longueur

1. 1/ 0 /1500
2. 1 / 185 /1500
3. 0 / 370 / 560

Soit M la taille du message, D = entête + M

- Si D > MTU => fragmentation :
  - Dans tous les paquets sauf le dernier, MF flag=1 (bit 2)
  - Mettre dans offset fragment, le nombre de blocs de 8 octets, soit i*floor(D/8), où i est le numéro de fragment (i=[0,….)

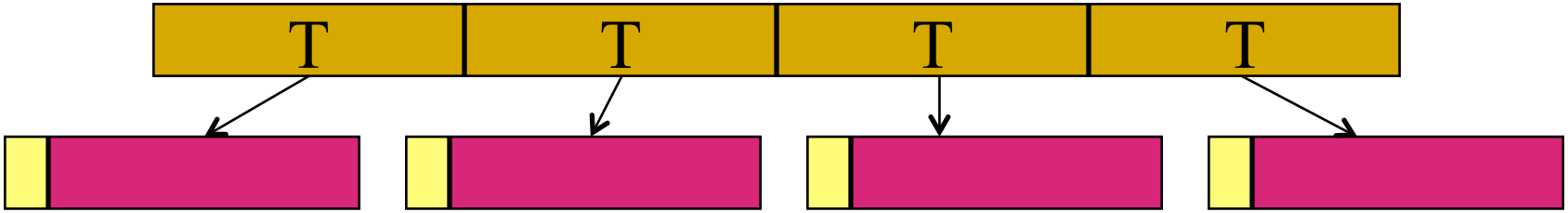
IP : Fragmentation



- identificateur du paquet (Id bits 0-15)
  - tous les fragments auront le même identificateur
- indicateurs (bits 16, 17, 18)
  - bit 16 : non utilisé
  - bit 17 : **DF** DO NOT FRAGMENT
  - bit 18 : **MF** MORE FRAGMENT
- déplacement (bits 19-31)
  - début du fragment par rapport au début du paquet
  - numéroté par groupe de 8 octets

INTERNET : fragmentation

T =MTU - entête



Id = X	Id = X	Id = X	Id = X
MF= 1	MF= 1	MF= 1	MF= 0
offset= 0	offset= T/8	offset= 2T/8	offset=3T/8

- réception dans le désordre
- en cas de perte d'un fragment, tout les paquets sont ignorés
- réassemblage par la destination

TCP (Transmission control Protocol)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Objectif : transmettre de manière fiable entre deux entités identifiées par une paire (adresse IP, port)
- Protocole **mode connecté :** établissement d'une session de communication (début, fin)
- Protocole **fiable**
  - somme de contrôle
  - contrôle de flux : fenêtres d'émission dont la taille est négociée avec le réceptionnaire
  - contrôle de congestion (Reno, Vegas, ...) : adaptation du débit aux conditions du réseau

Note : dans TCP, le contrôle de congestion dirige le contrôle de flux.

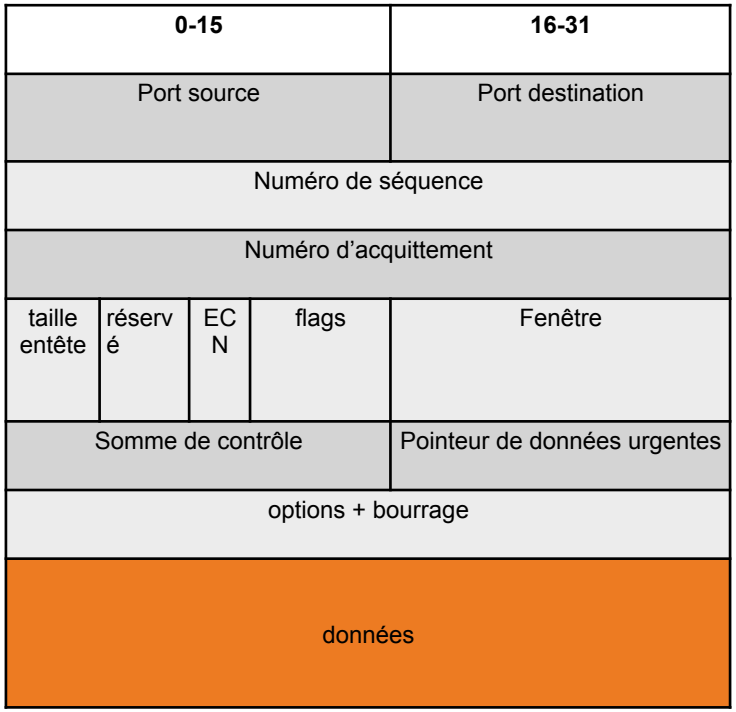
Segment TCP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

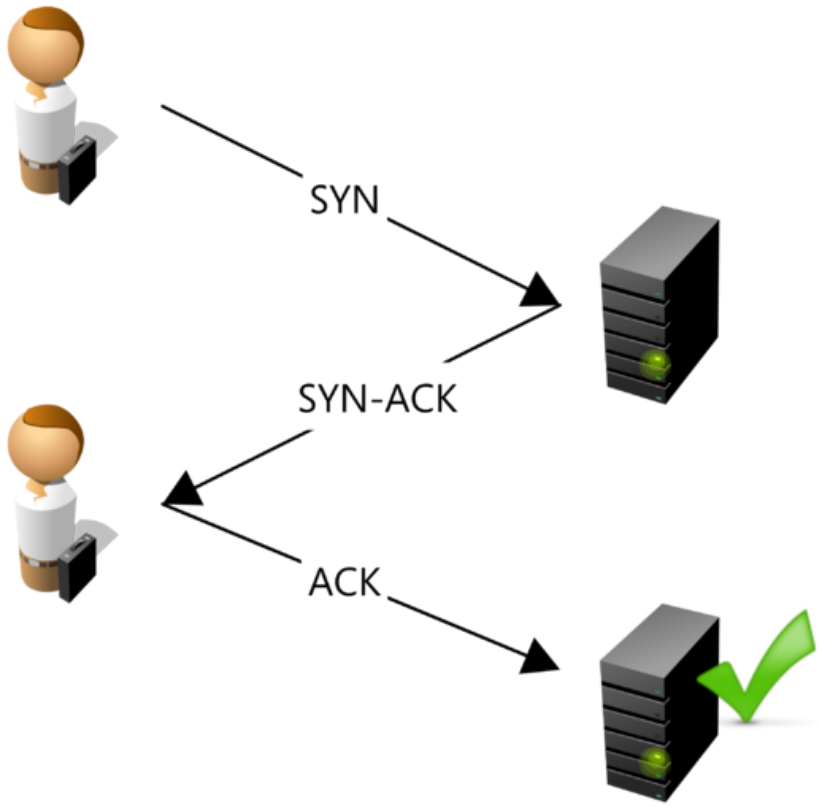
<table>
<tr><th colspan="4">0-15</th><th>16-31</th></tr>
<tr><td colspan="4">Port source</td><td>Port destination</td></tr>
<tr><td colspan="5">Numéro de séquence</td></tr>
<tr><td colspan="5">Numéro d’acquittement</td></tr>
<tr><td>taille entête</td><td>réservé</td><td>ECN</td><td>flags</td><td>Fenêtre</td></tr>
<tr><td colspan="4">Somme de contrôle</td><td>Pointeur de données urgentes</td></tr>
<tr><td colspan="5">options + bourrage</td></tr>
<tr><td colspan="5">données</td></tr>
</table>

Segment TCP

- Ports sources et destination (voir plus loin)
- N° séquence du 1er octet de ce segment
- N° acquittement: n° de séquence du prochain octet attendu
- taille entête en mots de 32 bits
- ECN : présence de congestion
- flags:
  - URG : 1 si données urgentes
  - ACK : 1 pour données acquittées
  - PSH : envoyer tout de suite
  - RST : reset sur la connexion
  - SYN : demande établissement connexion
  - FIN : demande fin connexion
- Fenêtre: taille demandée en octets



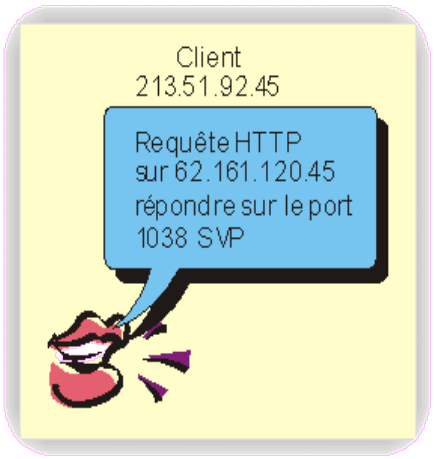
Session TCP

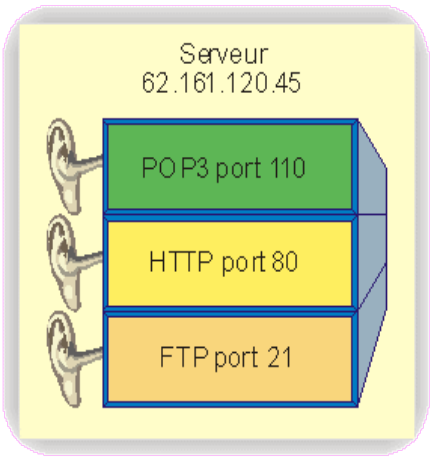


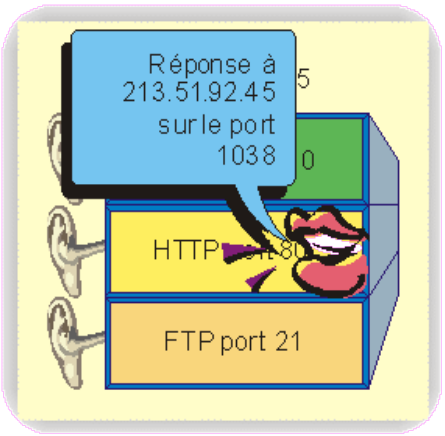
Ports et sockets

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Comment s'adresser à un service particulier sur une même machine ?







- Port + IP = socket
- Remarques
  - Un client peut dialoguer avec plusieurs services en même temps
  - Les services doivent utiliser des ports conventionnels (IANA)

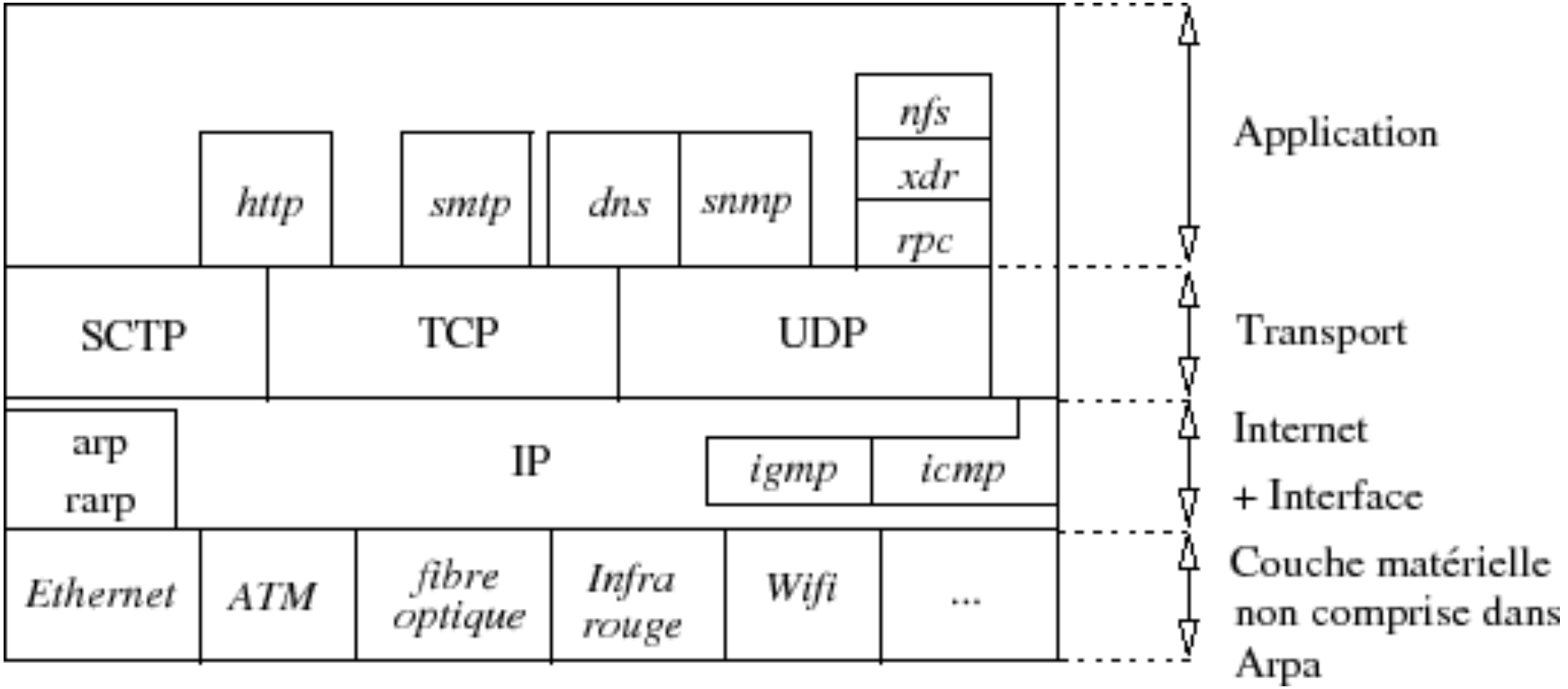
Numéros de ports : conventions

http://www.iana.org/assignments/port-numbers

(linux utilise la liste `/etc/services`)

Service	port
ftp	21
ssh	22
telnet	23
smtp	25
http	80
pop3	110
imap	143
imaps	993

La pile de protocoles usuels



UDP (User Datagram Protocol)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Objectif : transmettre de manière simple entre deux entités identifiées par une paire (adresse IP, port)
- Contrairement à TCP,
  - UDP est en mode non-connecté : pas de notion de session.
  - UDP est non-fiable :
  - pas de contrôle de flux : fenêtres d'émission dont la taille est négociée avec le réceptionnaire
  - pas de contrôle de congestion

Datagramme UDP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

0-15	16-31
Port source	Port destination
longueur	Somme de contrôle
données	

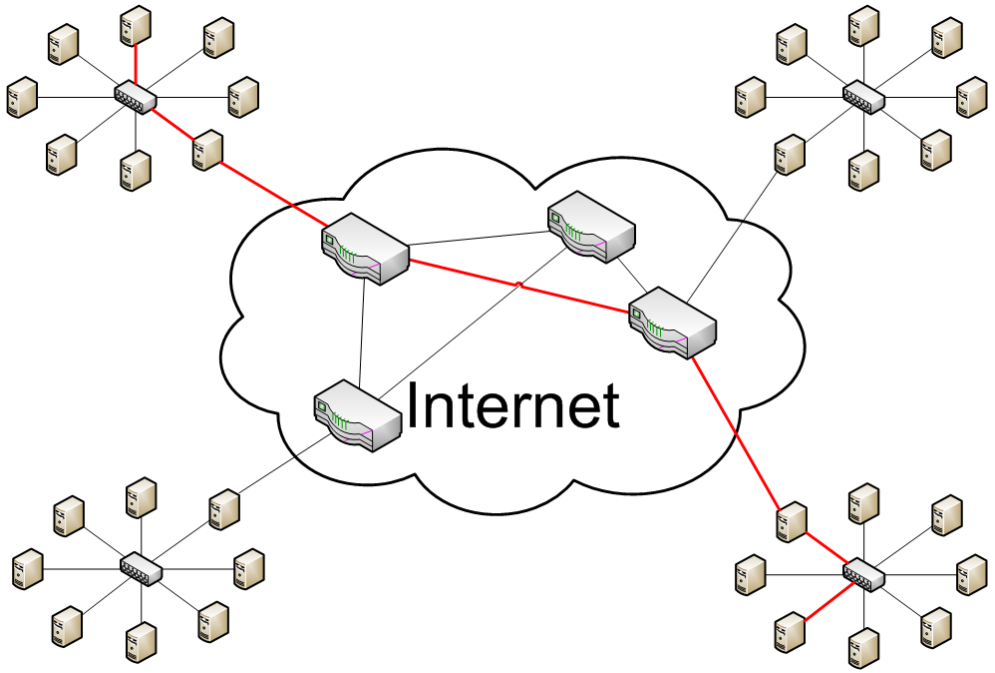
ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

Partie 2 : TCP/IP

Adresses IP, classes de réseaux, masques, résolution ARP, DNS.

Adressage IP

- Objectif : communiquer avec un équipement hors de son réseau local => nécessite de le localiser et router messages jusqu'à lui



Adressage IP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Chaque matériel réseau possède un identifiant unique sur internet : son adresse IP
- Le numéro IP reflète la localisation du matériel.
- Sa forme : 4 octets, notée habituellement en décimal.
  - Exemple 192.132.12.165
- Attribué par l'administrateur réseau dont le matériel dépend.
  - Un particulier l'obtient de son FAI
- Mode d'attribution :
  - Fixe ou dynamique (donné par DHCP, valable pendant la connexion)

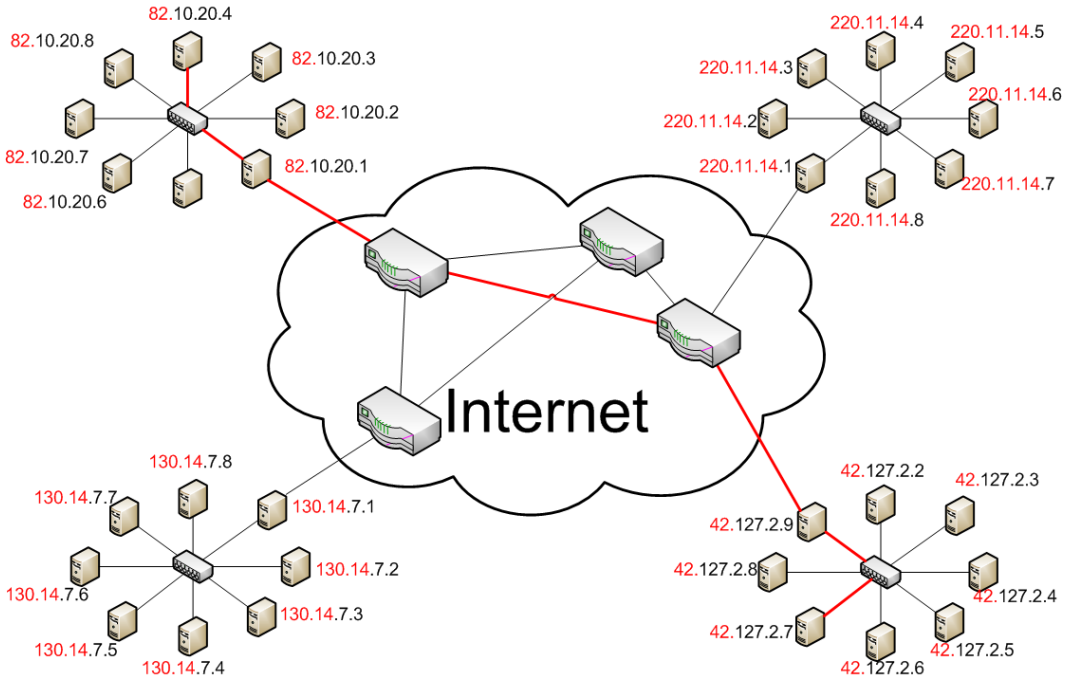
Attribution adresse IP

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Attribution d'une IP: gestion hiérarchique
  - Instance internationale ICANN chargée de la gestion
  - Délègue auprès d'instances régionales (Internet Registries)
    - APNIC (Asie-Pacifique)
    - ARIN (Amérique du Nord)
    - RIPE NCC (Europe)
  - Les instances régionales accordent une plage à des instances locales (FAI, grandes entreprises,...)
    - Environ 200 en France
    - Les administrateurs réseaux de ces LIR distribuent des numéros aux utilisateurs

Adressage IP

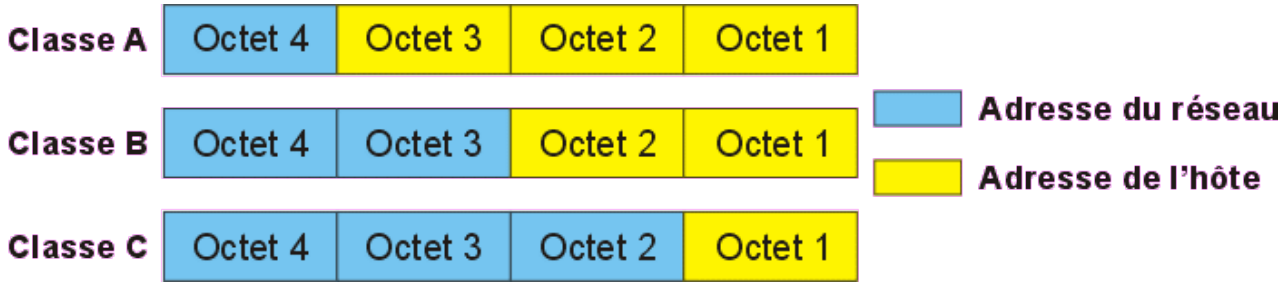
- L'adresse IP à une signification « variable »
  - Chaque administrateur réseau doit choisir la part du numéro IP qui désignera
    - Le réseau
    - La machine (l'hôte)



Adressage IP : classes de réseau

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Les répartitions types sont appelées classes de réseau
- La classe peut être déterminée à partir des 3 premiers bits
  - classe A : commence par 0 : [0.0.0.0,127.255.255.255]
  - classe B : commence par 10 : [128.0.0,191.255.255.255]
  - classe C : commence par 110 : [192.0.0.0,223.255.255.255]



Adresses IP spéciales

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Boucle locale (loopback) : 127.0.0.1
- Adresses privées
  - classe A : 10.0.0.0
  - classe B: 172.16.0.0 à 172.31.0.0
  - classe C: 192.168.0.0 à 192.168.255.0
- Adresse broadcast, multicast
  - broadcast : 255.255.255.255
  - multicast : 255.x.x.x

Masques

- On utilise un masque de réseau (netmask) pour séparer de manière simple la partie hôte de la partie réseau.
  - réseau= adresse ET masque
  - hôte = adresse ET (complément à 1 (masque))
- Pour les classes prédéfinies
  - masque classe A : 255.0.0.0
  - masque classe B : 255.255.0.0
  - masque classe C: 255.255.255.0

Masques (2)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Exemple:

adresse :212.27.63.122 masque: 255.255.255.0

	adresse	212	27	63	122
	adresse	11010100	00011011	00111111	01111010
	masque	11111111	11111111	11111111	00000000
adresse & masque	réseau	11010100	00011011	00111111	00000000
	!masque	00000000	00000000	00000000	11111111
adresse & !masque	hôte	00000000	00000000	00000000	01111010

Masques (3)

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

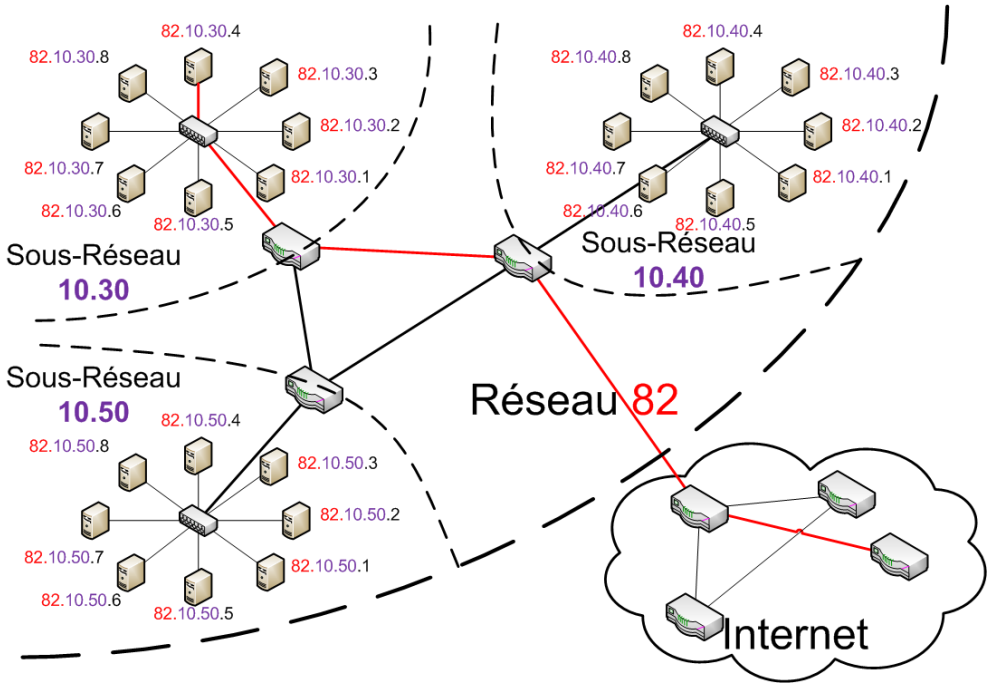
- Le découpage en classes (grain: l'octet) est rigide.
- Un mode de découpage plus général (au niveau du bit) est exprimée par **CIDR**
  - La notation CIDR est concise: de la forme `addr/len`

  où len est le nombre de bits utilisés pour le réseau.
  - Par exemple `212.27.63.122/19` signifie

  l'adresse IP 212.27.63.122 avec masque réseau
  `11111111.1111111.11100000.00000 (binaire)`
  ou `255.255.255.224.0 (décimal)`
    - Il reste donc 32-19=13 bits pour les hôtes
    - dans l'exemple, l'hôte est `0.0.31.122`

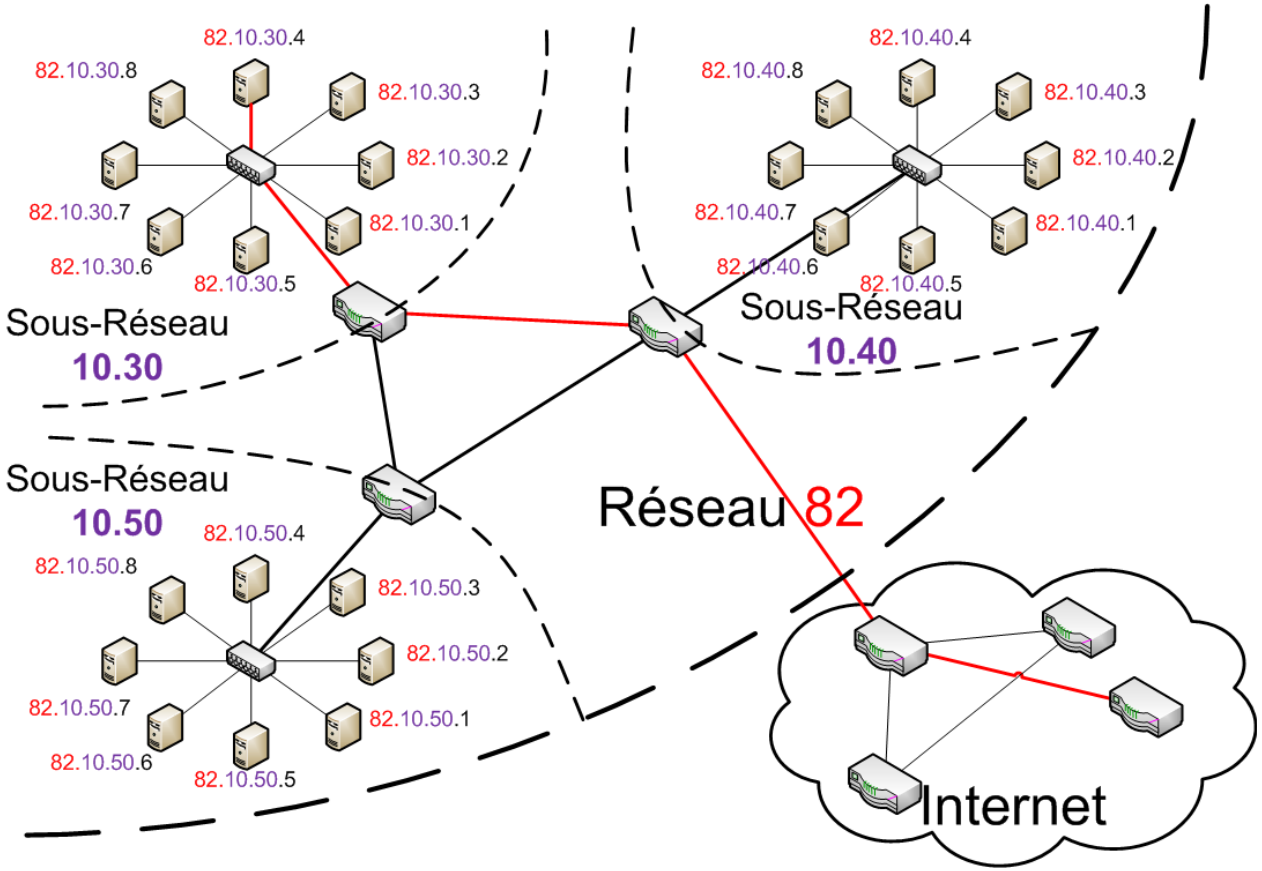
Routage

- L'adresse IP permet de faire du routage
  - Connaissant la classe, le système détermine rapidement où envoyer le paquet.



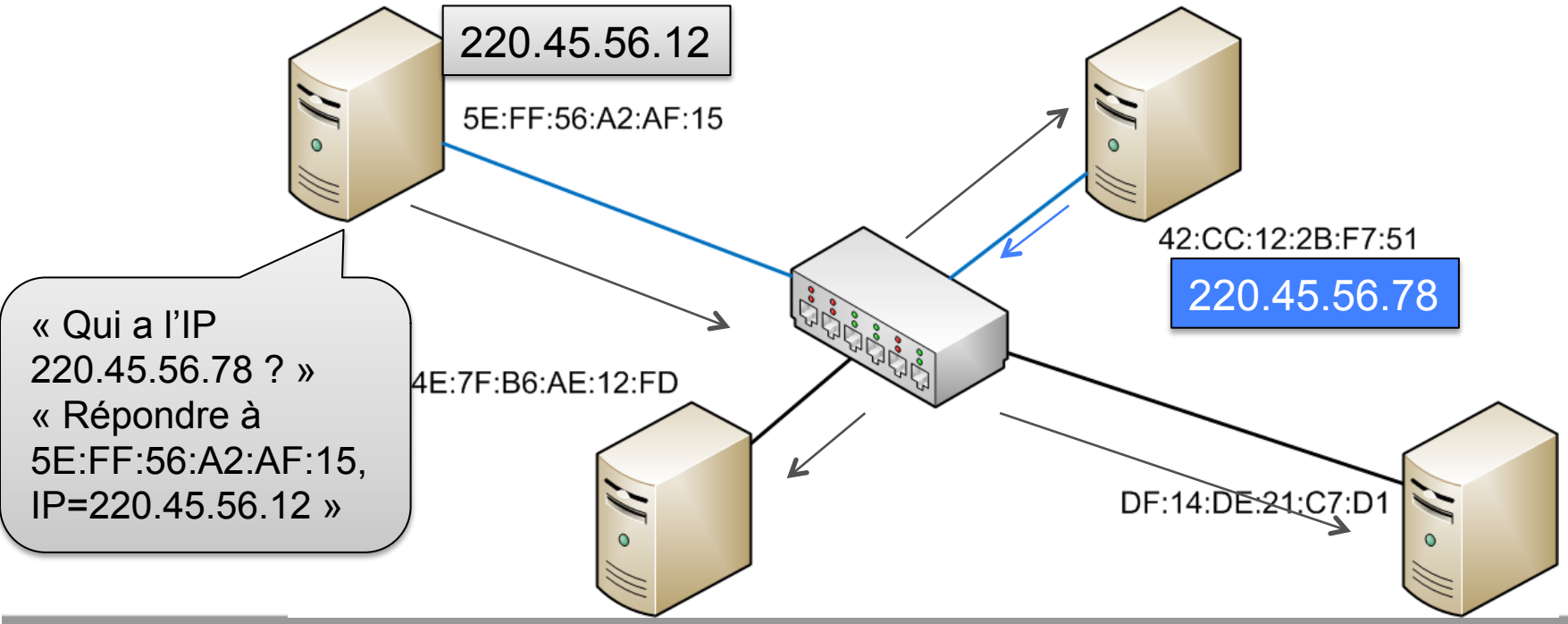
Routage

- Les réseaux sont découpés en sous-réseaux



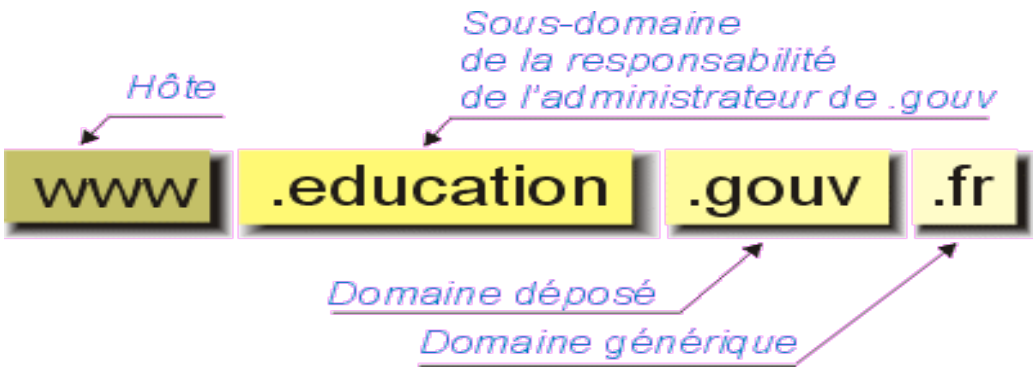
ARP

- ARP (Address Resolution Protocol) traduit
  - adresse de couche réseau (IPv4) vers
  - adresse de couche liaison (ethernet)



Le DNS - principe

- Les humains préfèrent les noms aux numéros
  - Nous utilisons avantageusement www.free.fr au lieu de 212.27.32.5
  - Le système DNS (Domain Name Server) assure la correspondance : service de résolution de noms.
    - [genaud@iso]$ nslookup www.free.fr
    - Address: 212.27.32.5
  - Le nom d'une machine suit des règles (FQDN). Le domaine générique est aussi appelé Top Level Domain (TLD).



Le DNS – configuration client

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Pour accéder au service du DNS, il faut que le système connaisse au moins l'IP d'une machine DNS:
  - Pour une IP fixe, la demander à l'administrateur réseau.
  - Pour les IP dynamique, le bail DHCP contient généralement l'adresse du DNS (transparent).
- C'est ce DNS qui prendra en charge toutes vos requêtes.
- On peut spécifier plusieurs DNS : serviront en cas de défaillance du premier.

Le DNS – mécanisme

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

- Le DNS auquel vous vous adressez ne connaît pas toutes les machines d'internet. Imaginez un système de millions de machines en perpétuel changement, et obtenir une réponse en quelques millisecondes.
- Il existe une « colonne vertébrale » de l'internet : 13 serveurs : A.root-servers.net, ... , M.root-servers.net identiques.

  (ftp://ftp.rs.internic.net/domain/named.root)
- Ces serveurs connaissent les serveurs DNS capables de donner des adresses pour un TLD donné .

Le DNS – mécanisme