UNIVERSITÉ
PARIS DESCARTES

Réseaux Informatiques

M. Hassine Moungla

B2-2

E-mail : Hassine.Moungla@parisdescartes.fr

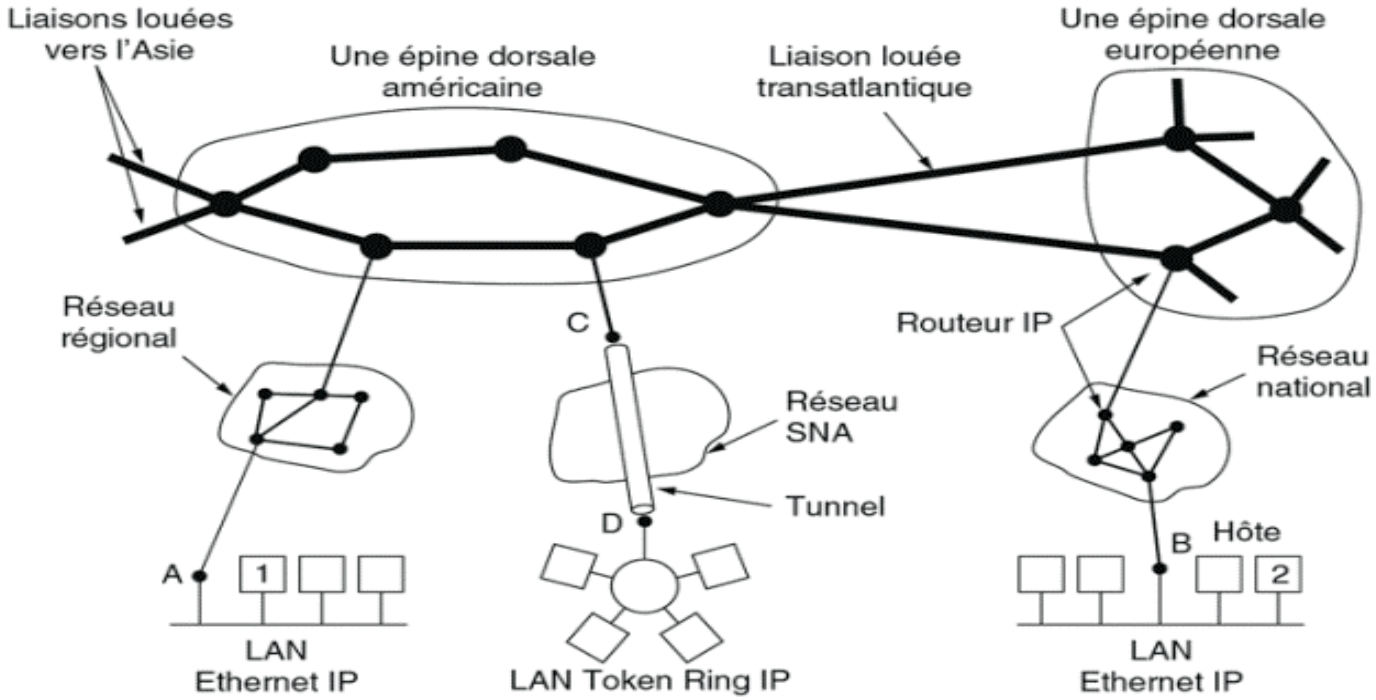
Couche Réseaux
Plan

1. Historique

- Architecture développée par la DARPA (Defence Advanced Research Project Adgency), milieu des années 1970
- IP : Internet Protocol - résout les problèmes d'interconnexion en milieu hétérogène (1974)
- TCP : Transmission Control Protocol - protocole de transport de l'Internet (de bout en bout)
- TCP/IP est intégré à Unix BSD 4 (Berkeley) en 1980
- TCP/IP est intégré à ARPANET en 1983
- Aujourd'hui, TCP/IP est devenu le standard d'Internet (Internet pour Inter-Networking)

l'Internet 1ère génération

- Un ensemble de sous-réseaux indépendants (Autonomous System) et hétérogènes qui sont interconnectés (organisation hiérarchique)



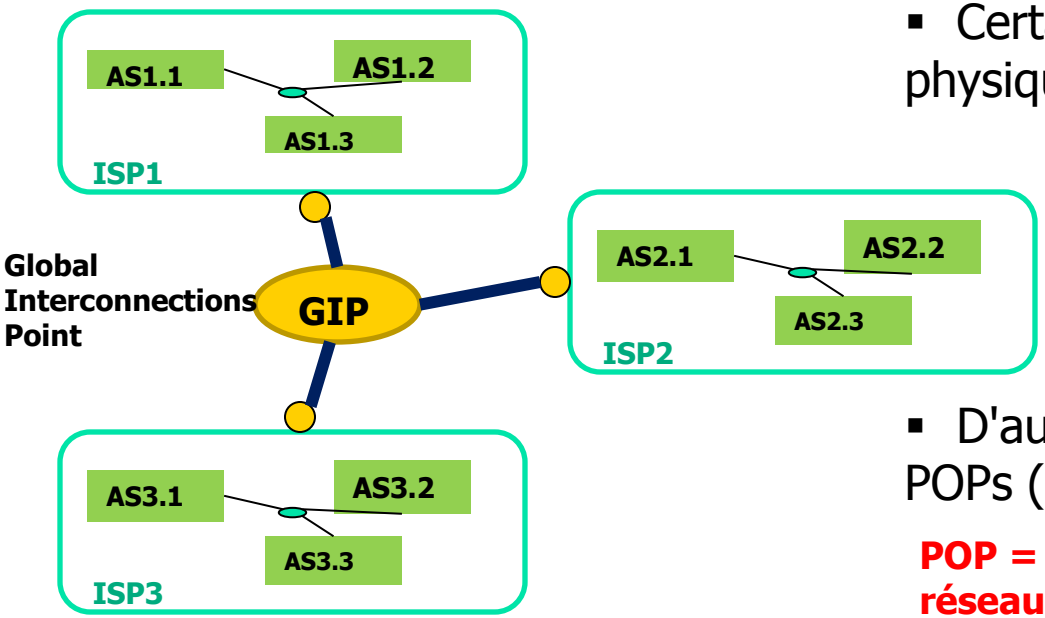
- S'articule autour deplusieurs backbone

l'Internet 2èmme génération

- Trois types de systèmes autonomes
  - les AS de transit (backbone) (réseaux régionaux,nationaux, …) qui acceptent de faire transiter despaquets d'autres AS
    - parfois avec certaines restrictions
    - souvent moyennant finance
  - les puits (stubs) : réseaux sans issue qui ne peuvent acheminer aucun trafic externe
  - les AS multi-connectés qui peuvent être utilisés pour du transit, sauf indication contraire (mais ce n'est pas leur rôle premier)
- **Peering :** accords de transit entre ISP -> point d'interconnexion privés

l'Internet 3ème génération

- ISP - Internet Service Provider
  - un ou plusieurs systèmes autonomes
  - un AS = ensemble de réseaux/routeurs sous la même autorité d'administration (entreprise, campus, …)

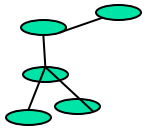


- Certains ISP ont une infrastructure physique de réseau (possèdent des lignes)
- D'autres proposent uniquement des POPs (Points of Presence)

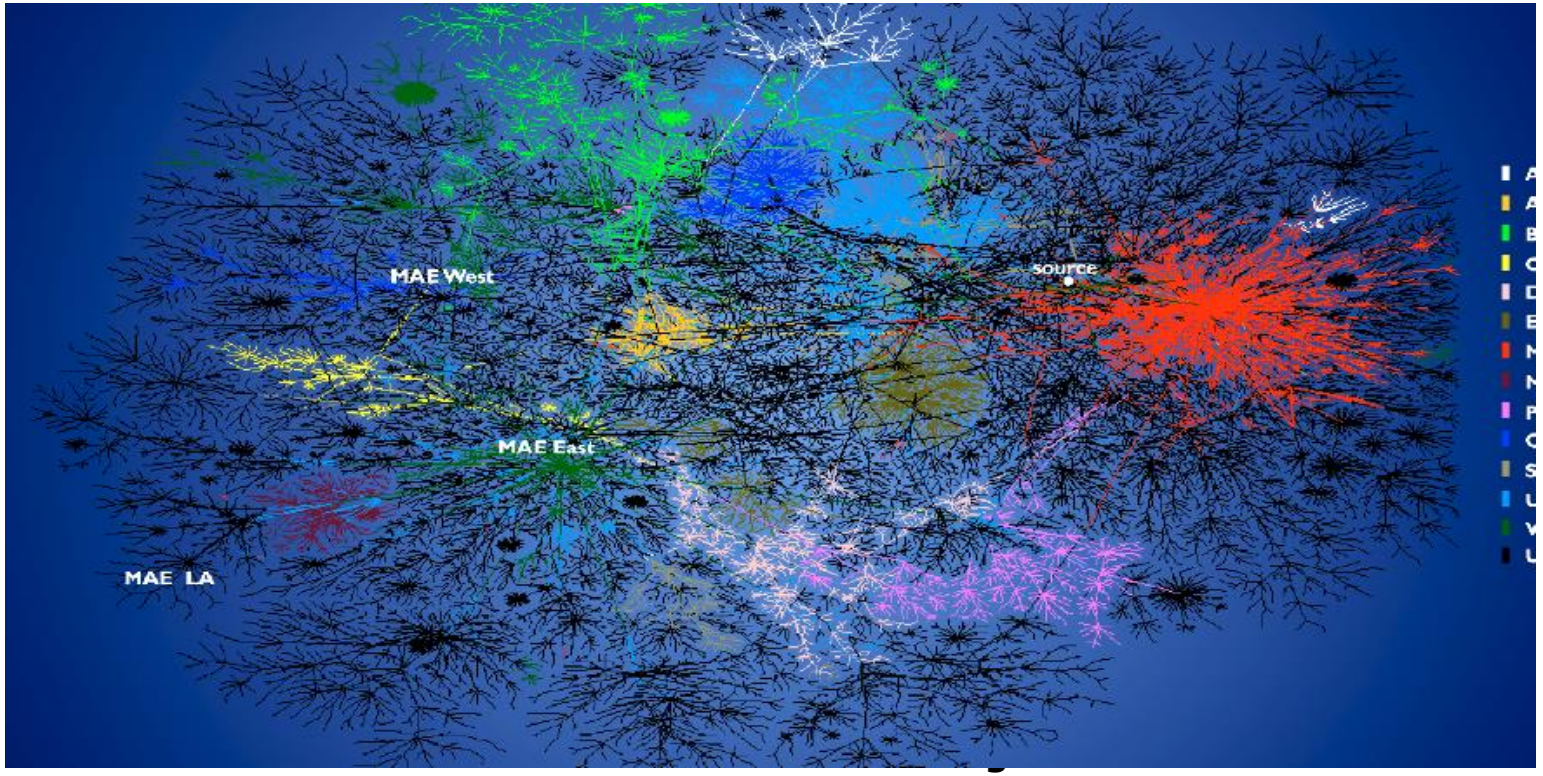
POP = interface entre le réseau d'accès et le réseau de transit

l'Internet suite ……génération

- **1969**

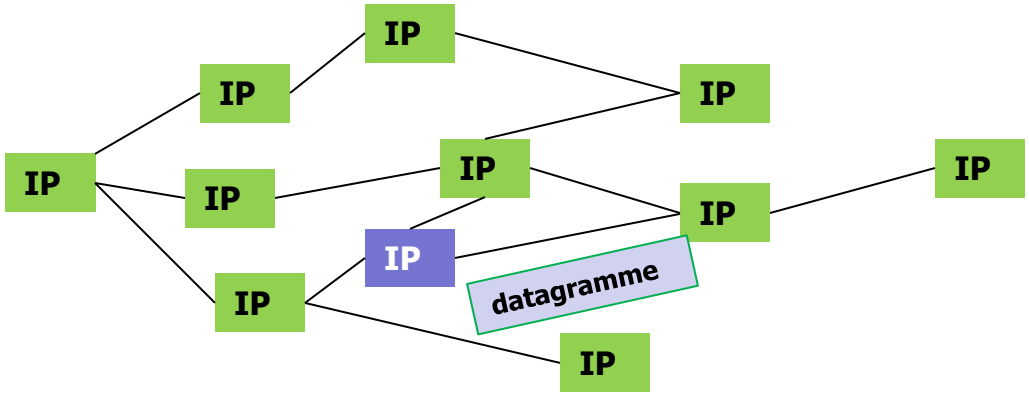


- **Le big-bang (US) 2003 : environ 200 millions de machines**



Fonctionnement de l'Internet

- **Couche réseau : communications entre machines**

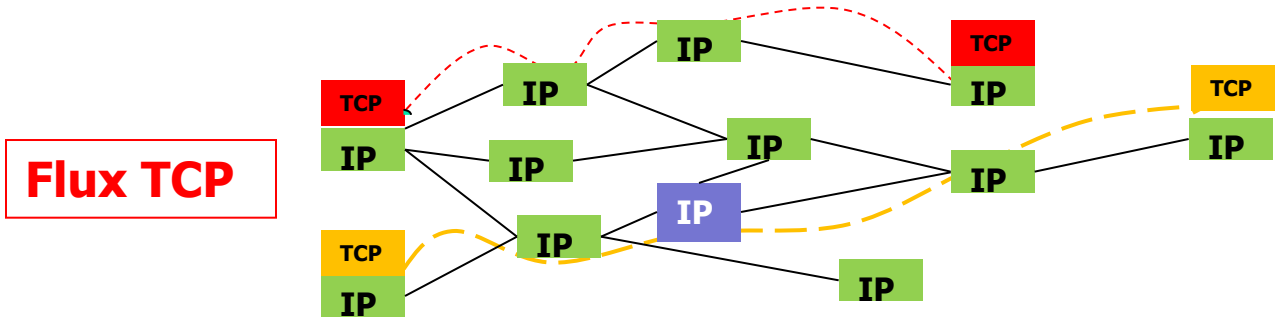


Noeud intermédiaire : routeur (matériel ou logiciel)

- IP - protocole d'interconnexion, best-effort
  - acheminement de **datagrammes (mode non connecté)**
  - peu de fonctionnalités, pas de garanties
  - simple mais robuste (défaillance d'un noeud intermédiaire)

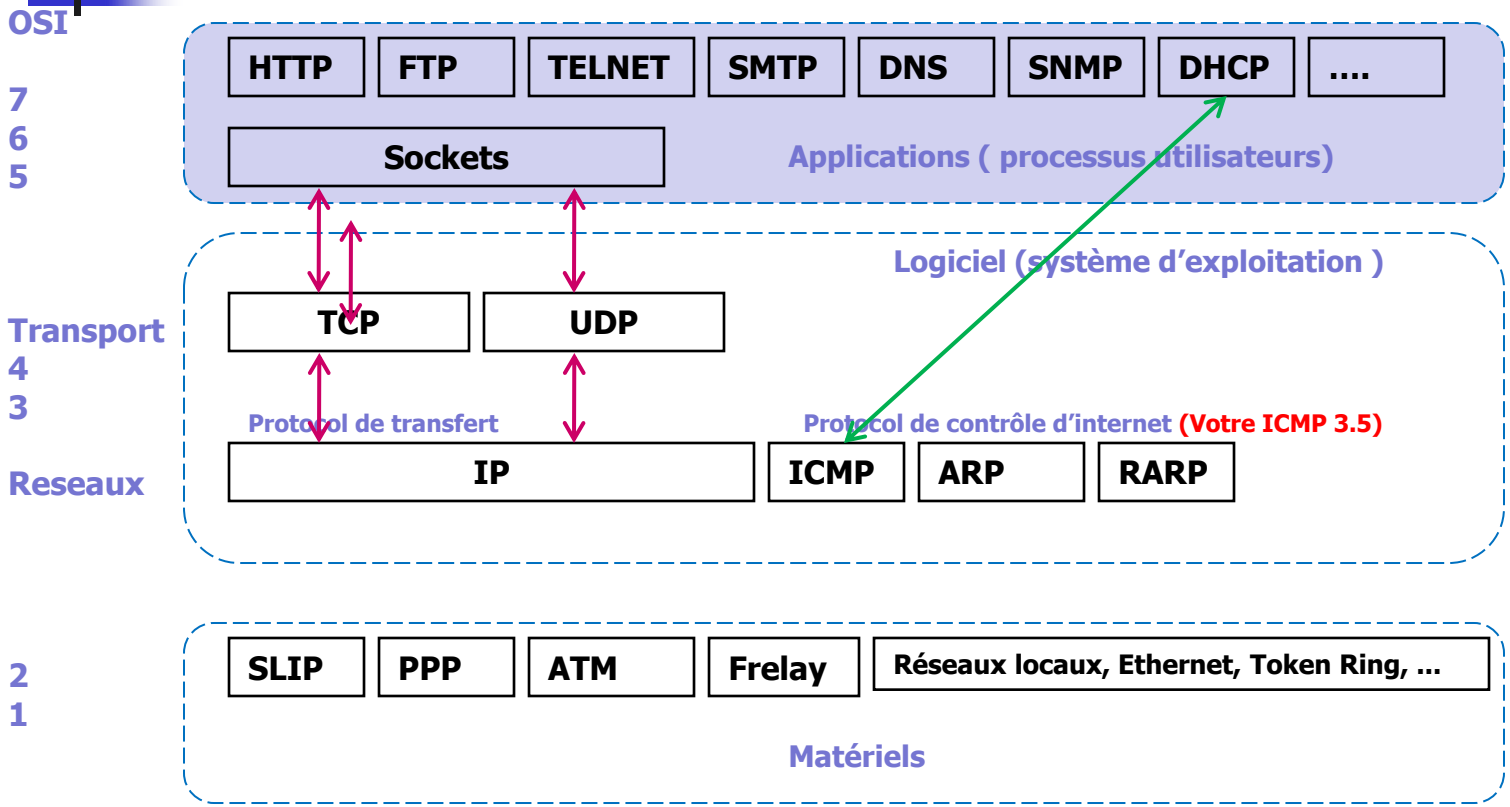
Fonctionnement de l'Internet

Couche transport : communications entre applications



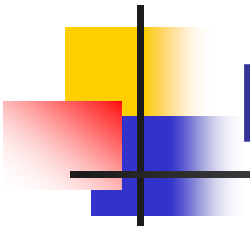
- **TCP - protocole de transport de bout en bout**
  - **uniquement présent aux extrémités**
  - **transport fiable de segments (mode connecté)**
  - **protocole complexe (retransmission, gestion des erreurs, séquencement, …)**

Architecture de TCP/IP



2.Protocoles et applications (1)

- Niveau applicatif
  - HTTP - HyperText Transport Protocol
    - protocole du web
    - échange de requête/réponse entre un client et un serveur web
  - FTP - File Transfer Protocol
    - protocole de manipulation de fichiers distants
    - transfert, suppression, création, …
  - TELNET - TELetypewriter Network Protocol
    - système de terminal virtuel
    - permet l'ouverture d'une session distante



Protocoles et applications (2)

- Niveau applicatif
  - SMTP - Simple Mail Transfer Protocol
    - service d'envoi de courrier électronique
    - réception (POP, IMAP, IMAPS, …)
  - DNS - Domain Name System
    - assure la correspondance entre un nom symbolique et une adresse Internet (adresse IP)
    - bases de données réparties sur le globe
  - SNMP - Simple Network Management Protocol
    - protocole d'administration de réseau (interrogation, configuration des équipements, …)
  - Les sockets - interface de programmation permettant
    - l'échange de données (via TCP ou UDP)

Protocoles et applications (3)

- Protocoles de transfert de données
  - TCP/IP : transfert fiable de données en mode connecté
  - UDP/IP : transfert non garanti de données en mode non connecté
- Protocoles de contrôle de l'Internet
  - ICMP - Internet Control and error Message Protocol
    - assure un dialogue IP<-->IP (entre routeurs par ex.) pour signaler les congestions, synchroniser les horloges, estimer les temps de transit, …
    - utilisé par l'utilitaire ping permettant de

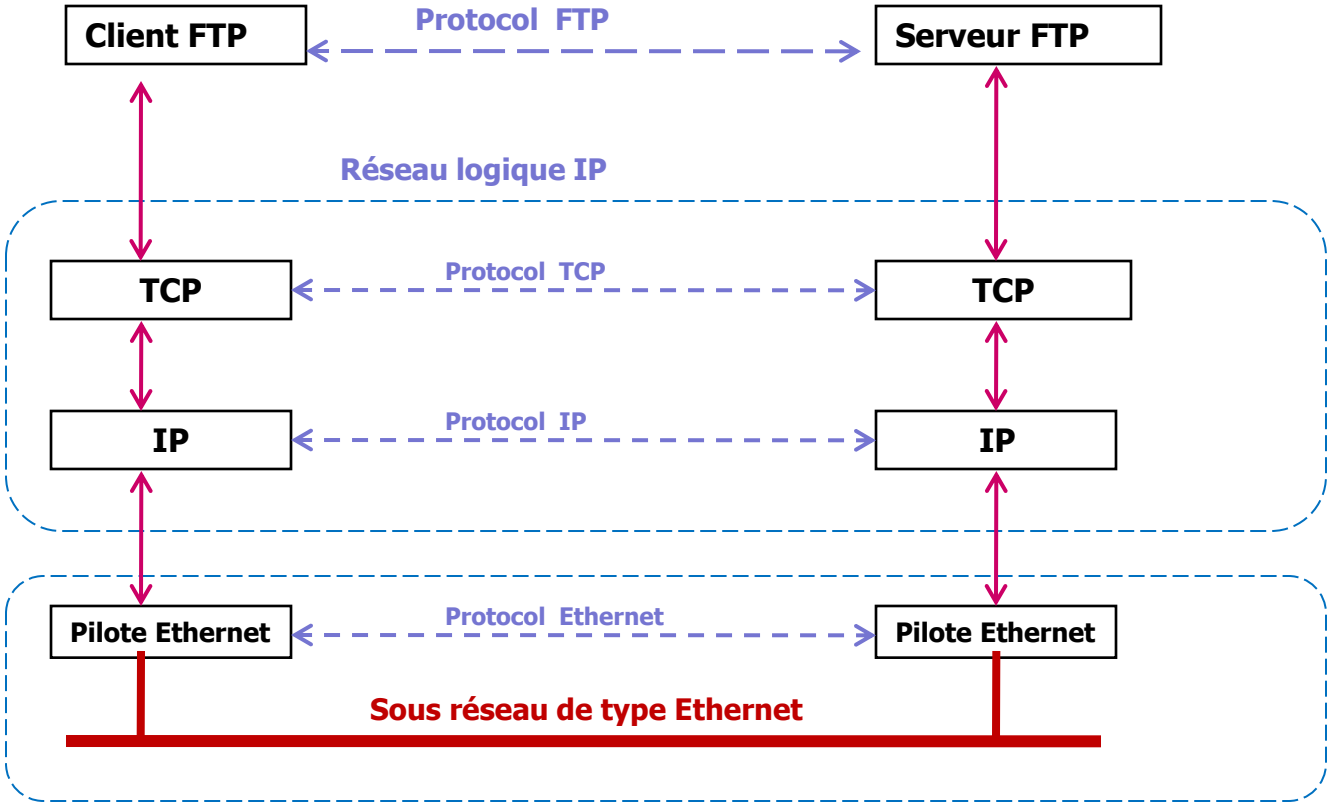
Protocoles et applications (4)

- Protocoles de contrôle de l'Internet
  - ARP - Address Resolution Protocol
    - protocole permettant d'associer une adresse MAC (adresse physique utilisée dans les réseaux locaux) à une adresse IP (adresse logique Internet)
  - RARP - Reverse ARP
    - permet à une station de connaître son adresse IP à partir de son adresse MAC (interrogation d'un serveur RARP)
  - phase de démarrage d'équipements ne possédant pas de configuration initiale (imprimante, terminal X)

Protocoles et applications (5)

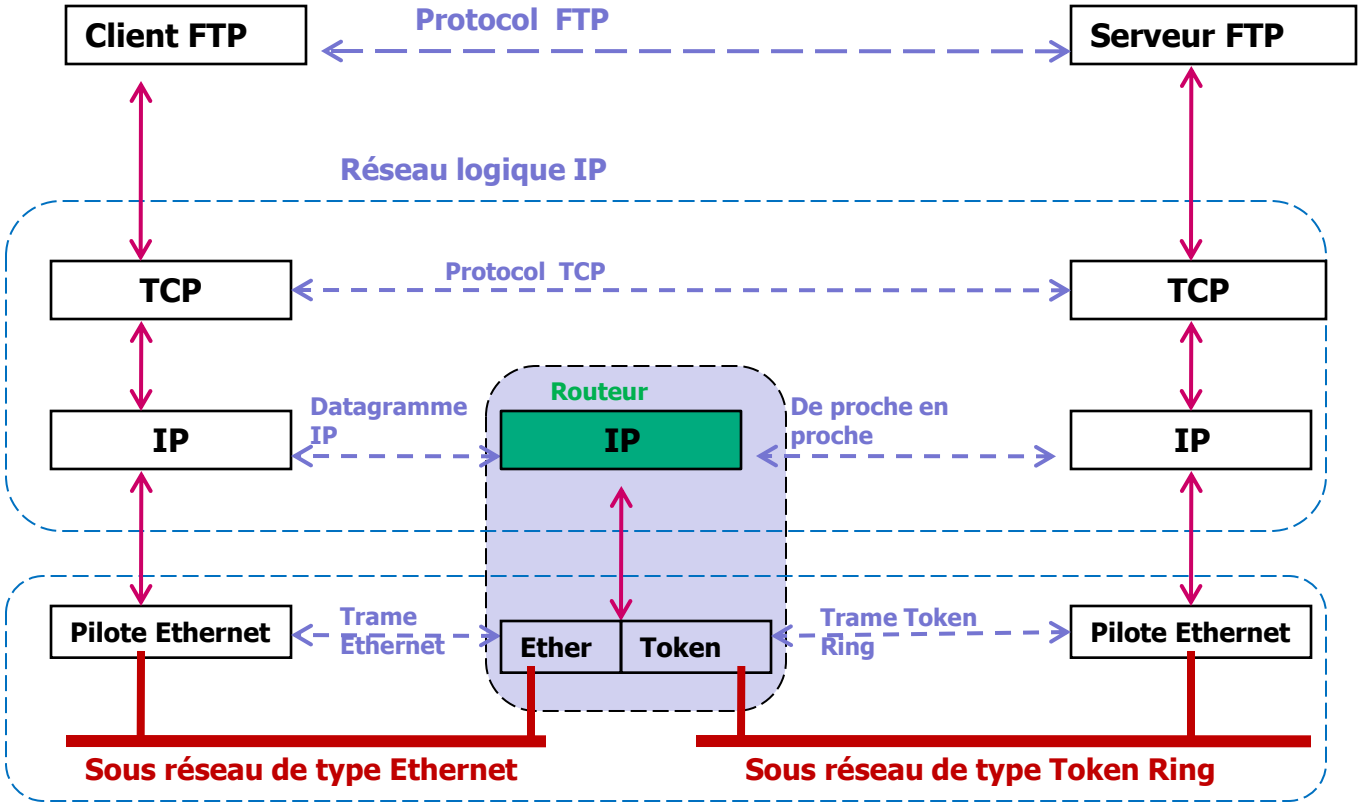
- Protocoles de contrôle de l'Internet
  - BOOTP - Boot Protocol
    - permet à une station de connaître sa configuration réseau lors du démarrage par interrogation d'un serveur bootp
    - au-dessus d'UDP (ports 67 et 68)
  - DHCP - Dynamic Host Configuration Protocol
    - extension du protocole BOOTP
    - meilleure gestion du plan d'adressage IP avec attribution dynamique des adresses IP pour une certaine durée (bail ou lease time)
    - au-dessus d'UDP (ports 67 et 68)

Communications sans routeur



Deux machines sur un meme sous réseaux

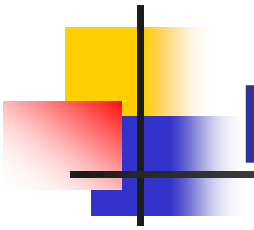
Communications avec routeur



prise en compte de l'Hétérogénéité

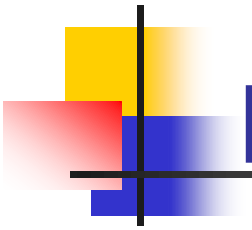
2.1. Le Protocole IP

- Le Protocole Internet ou **IP (Internet Protocol)** est la partie la plus fondamentale d'Internet.
- IP est une norme TCP/IP obligatoire définie dans la RFC 791, « Internet Protocol (IP) ».
- IP est un protocole de datagramme sans connexion instable principalement responsable des paquets d'adressage et de routage entre les hôtes.



Le Protocole IP

- Sans connexion signifie qu'aucune session n'est établie avant l'échange des données.
- Instable signifie que la livraison n'est pas garantie.



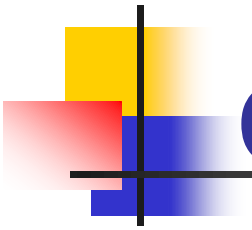
Le Protocole IP

- IP fait toujours de son mieux pour livrer un paquet.
  - Un paquet IP peut être perdu, livré désynchronisé, répliqué ou retardé.
- IP ne tente pas de récupérer ces types d'erreurs.
  - L'accusé de réception des paquets livrés et la récupération des paquets perdus sont du ressort d'un protocole de couche supérieure tel que le protocole TCP.

Couche réseau dans l'Internet

Fonctions de IP

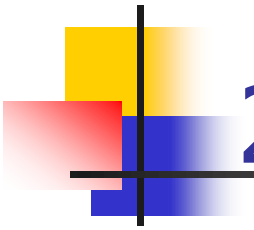
- Acheminement des Datagrammes vers un destinataire en mode non connecté
  - @IP (adresse IP)
- Routage : déterminer le chemin
  - Pour les paquets de la couche Transport
  - Pour les trames de la couche Liaison (router)
  - Aucune connaissance du réseau Internet
- Fragmentation/ Réassemblage
- Gestion des options IP
- Envoi et réception des messages de contrôle de ICMP



Couche réseau dans l'Internet

Ce que IP ne fait pas

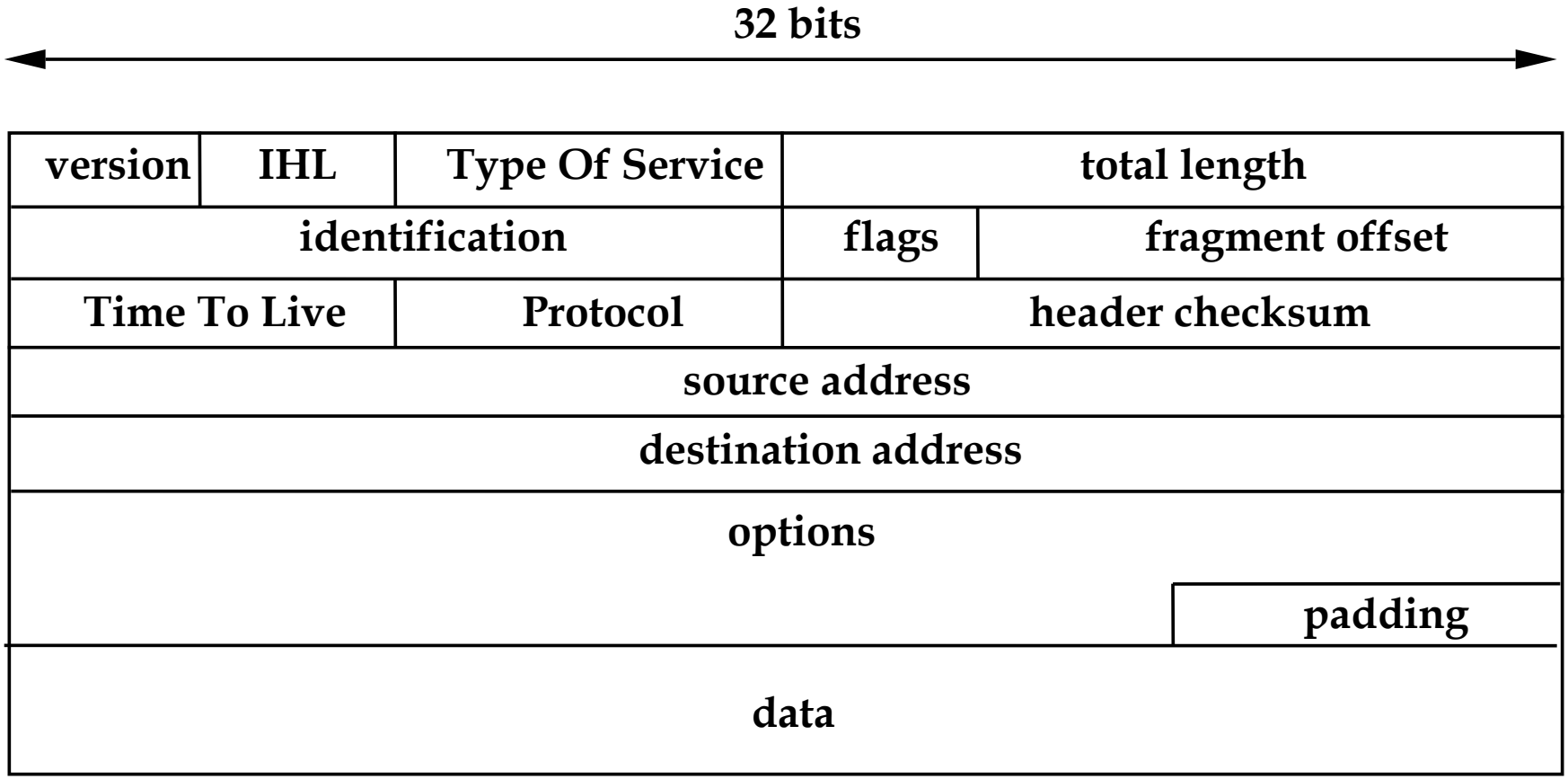
- **IP n'est pas fiable : il ne fait pas de :**
  - Multiplexage
  - Séquencement
  - Détection des duplications
  - Détection des pertes et retransmission
  - Contrôle de flux
- **IP est un protocole « Best Effort »**

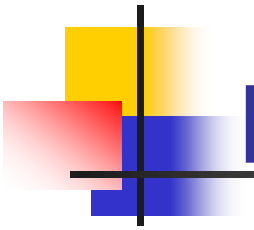


2.2. Adressage IP

- Le datagramme IP
- Pourquoi un subnet sur un LAN ou WAN, MAN ?
- Quelles adresses TCP/IP utiliser ?
  - Les classes d'adresses
  - Les adresses TCP/IP réservées ("privées")
  - Le masque de réseau
- La création d'un sous-réseau
  - Les masques du sous-réseau
  - Les adresses de diffusion (broadcast)
  - Exemple avec un réseau classe C
- Adressage CIDR

Le datagramme IP





Le datagramme IP

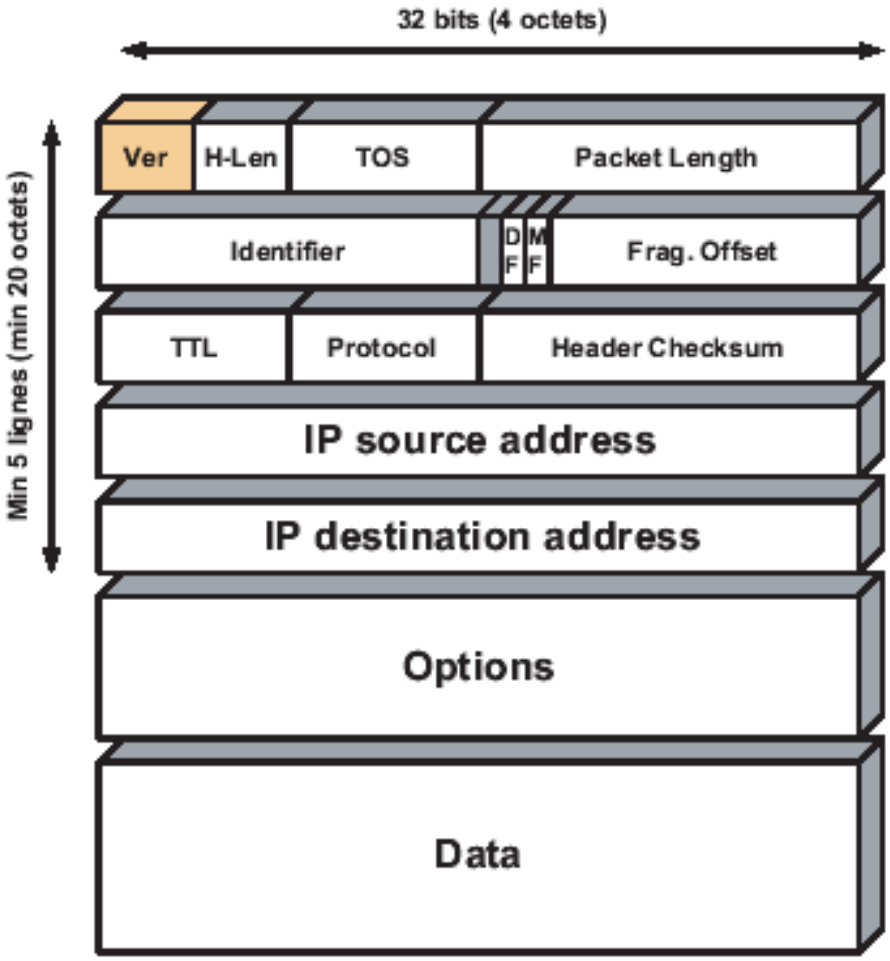
- Les paquets IP sont constitués d'un en-tête contenant l'adresse IP de l'expéditeur (votre ordinateur) et celle du destinataire (l'ordinateur que vous voulez atteindre),

- ainsi qu'un nombre de contrôle déterminé par l'information emballée dans le paquet :
  - ce nombre de contrôle, communément appelé *en-tête de total de contrôle*, permet au destinataire de savoir si le paquet IP a été "abîmé" pendant son transport.

Le datagramme IP

- L'en-tête IP est alignée sur des mots de 32 bits. Sa longueur est donc multiple de 4 octets. Par défaut, sans option, l'en-tête IP fait 20 octets de long
  - « Version » indique le format de l'en-tête. Ce champ sert à l'identification de la version courante du protocole. La version décrite ici (et aujourd'hui utilisée) porte le n°4
  - « IHL (IP Header Length) » est la longueur de l'en-tête IP exprimée en mots de 32 bits (5 au minimum)

Le datagramme IP : champ Version

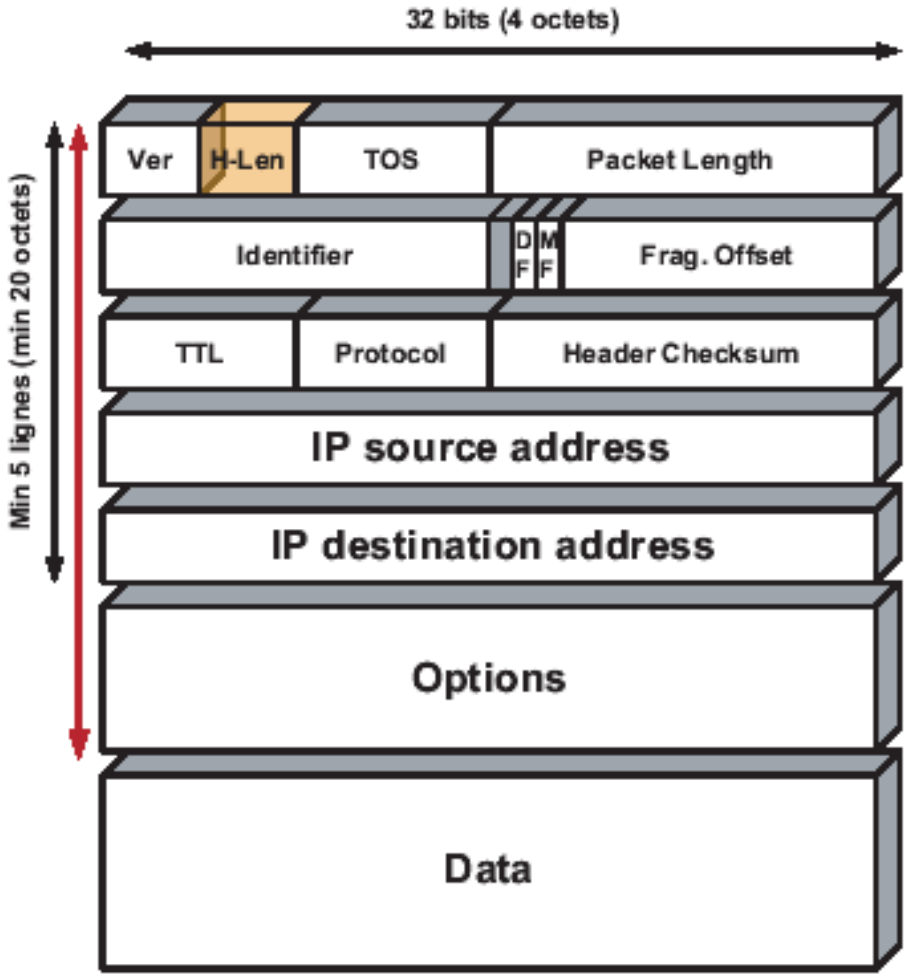


IP actuel : Version 4

IP next generation : Version 6

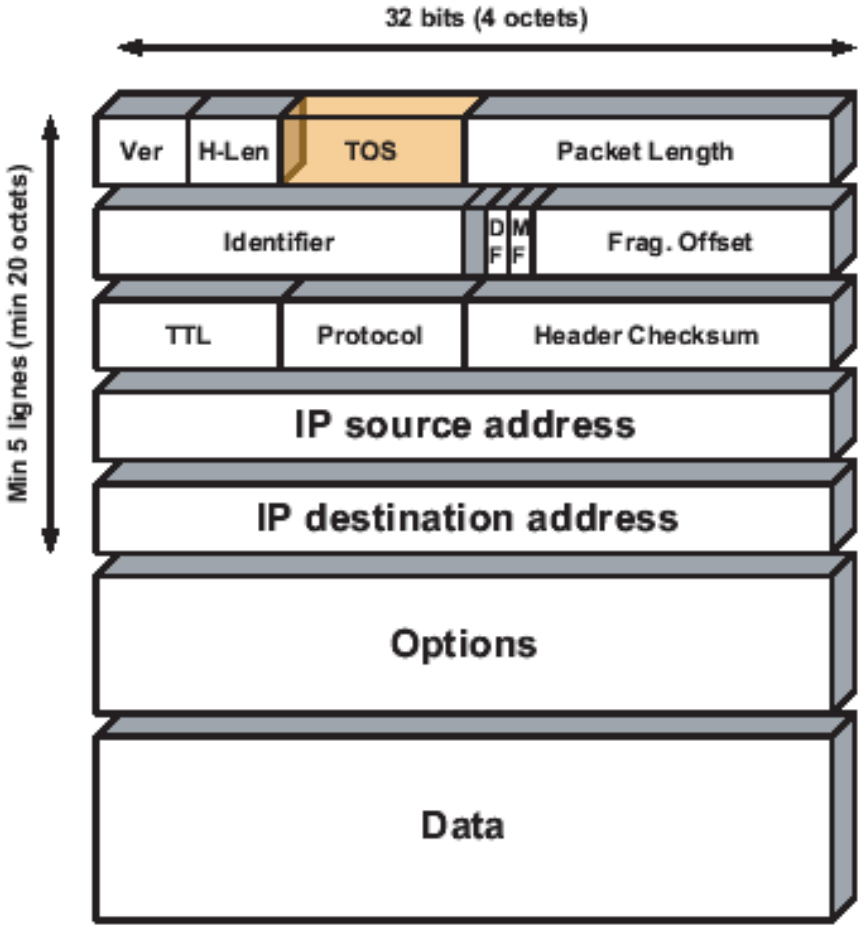
4 bits

Le datagramme IP : champ HLen



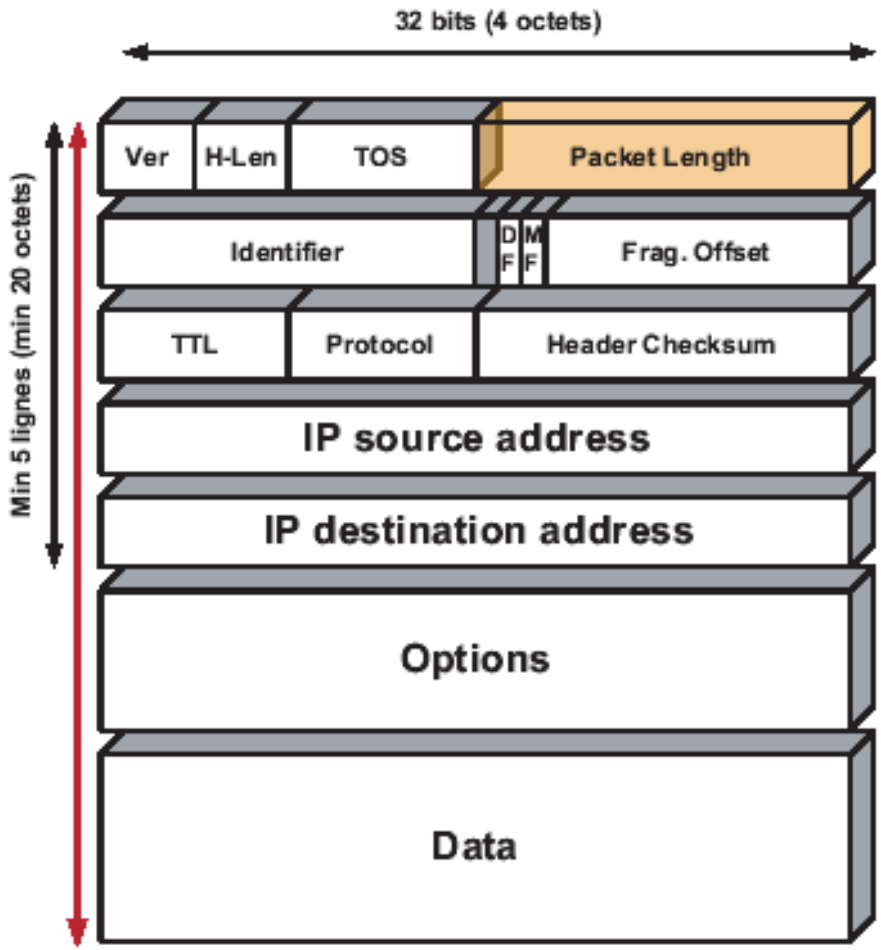
- nombre de lignes de 32 bits dans l'entête IP
- nécessaire car le champ option est de longueur variable (20 a 60 octets)
- valeur de : 5 (pas d'option) à 15 (10 lignes d'options, soit 40 octets)
- 4 bits (valeur "0" à "15" maximum)

Le datagramme IP : champ TOS



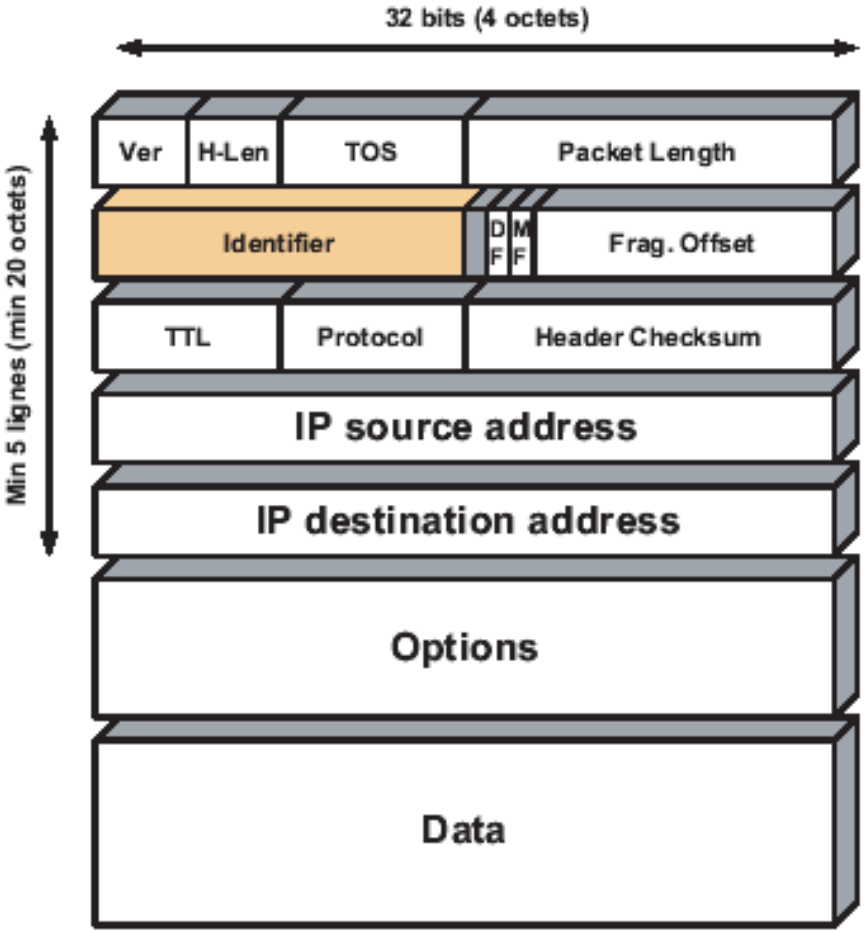
- 8 bits :
  - 3 bits de **priorité** (precedance)
    - ✓ 000 : *Routine*
    - ✓ 001 : *Priority*
    - ✓ 010 : *Immediate*
    - ✓ 011 : *Flash*
    - ✓ 100 : *Flash override*
    - ✓ 110 : *Internetwork control*
    - ✓ 111 : *Network control*
  - 3 bits de **service**
    - ✓ *Delay*
    - ✓ *Throughput*
    - ✓ *Reliability*
    - ✓ *(cost)*
- non utilisé pour le moment

Le datagramme IP : champ packet length



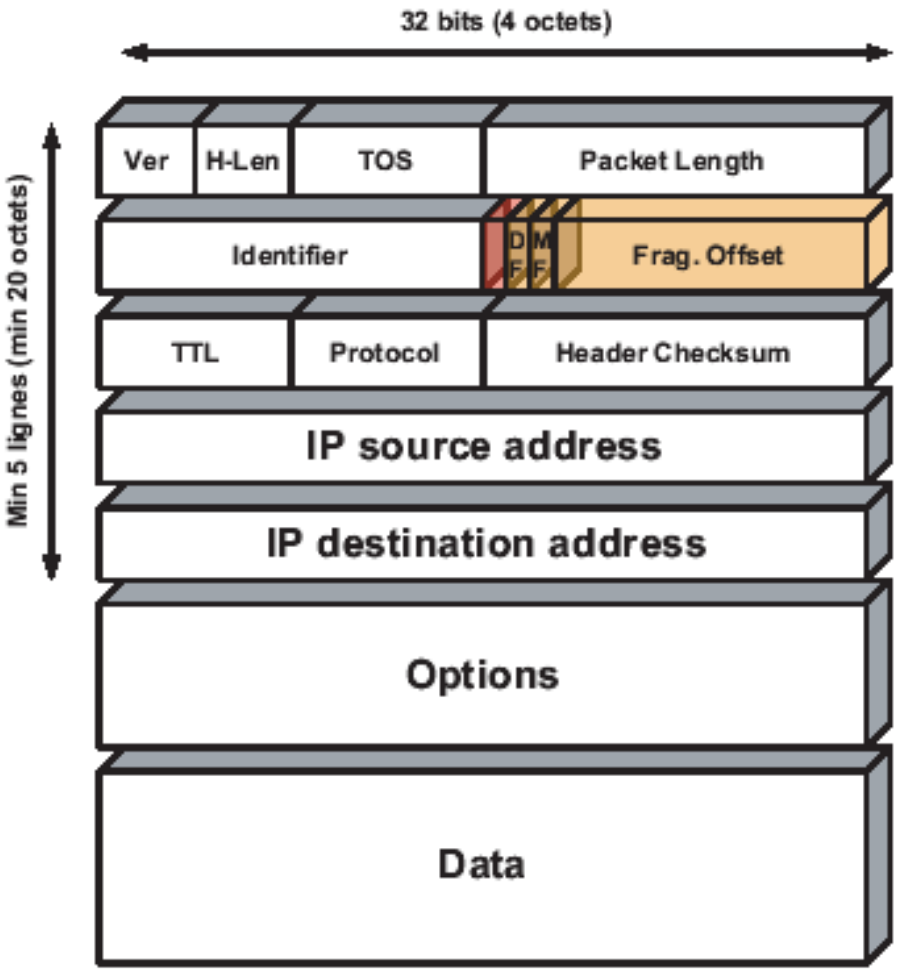
- taille totale du paquet avec entête
- exprimé en octets
- 16 bits (64 K-octets maximum)

Le datagramme IP : champ identification



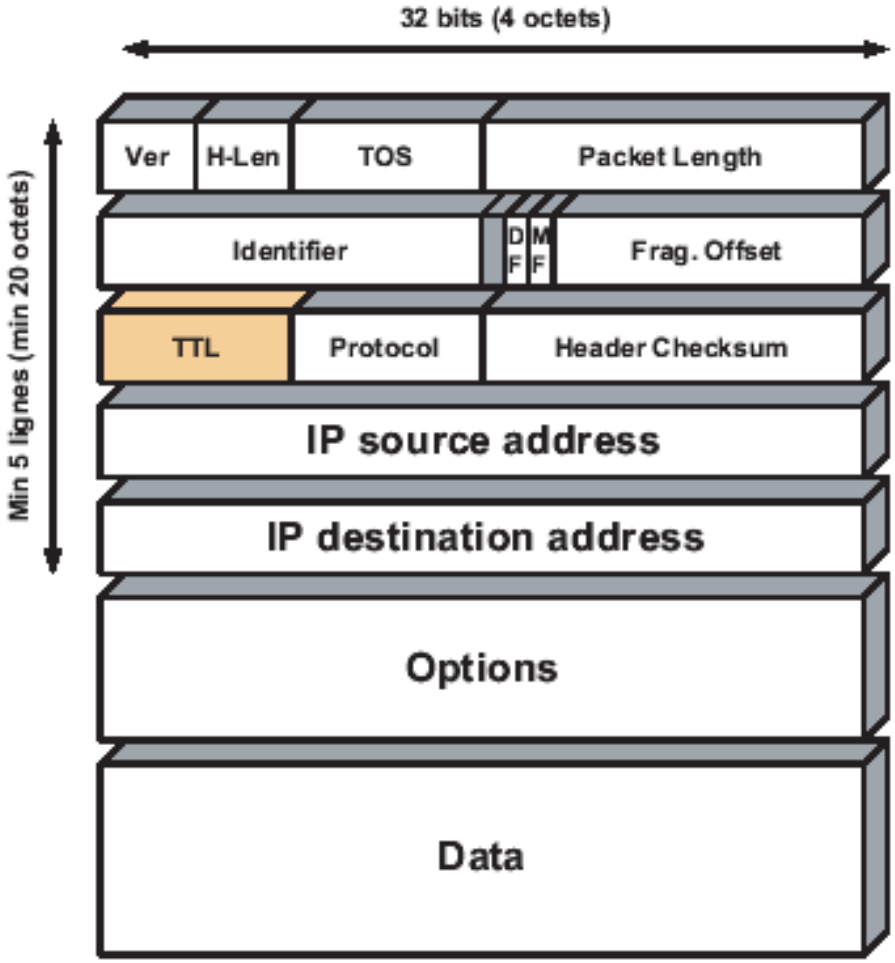
- défini de manière unique pour chaque paquet
- pour réassembler les fragments d'un même paquet
- habituellement, incrément d'un compteur pour chaque paquet successif
- 16 bits (boucle tous les 64 K paquets)

Le datagramme IP : champ frag-Offset



- 1 bits réservé
- 1 bits DF : Don't Fragment (=1 interdit la fragmentation)
- 1 bit MF : More Fragment (=0 pour le dernier fragment)
- 13 bits fragment offset en octets/8

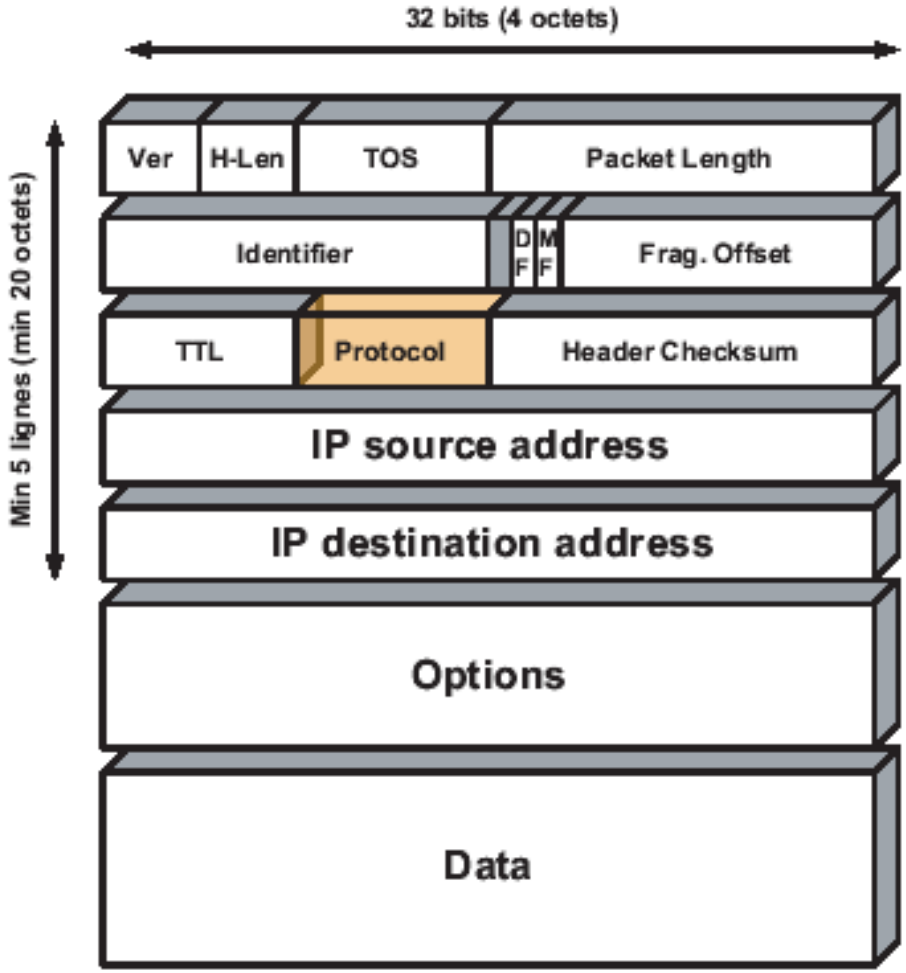
Le datagramme IP : champ TTL



Time To Live

- unité initiale : seconde
- valeur maximale fixé par l'émetteur (255, 128, 64, ...)
- décrément dans chaque routeur
- minimum 1 par routeur ⇛ nombre de sauts
- évite les boucles
- 8 bits (maximum 255 secondes ou sauts)

Le datagramme IP : champ Protocol



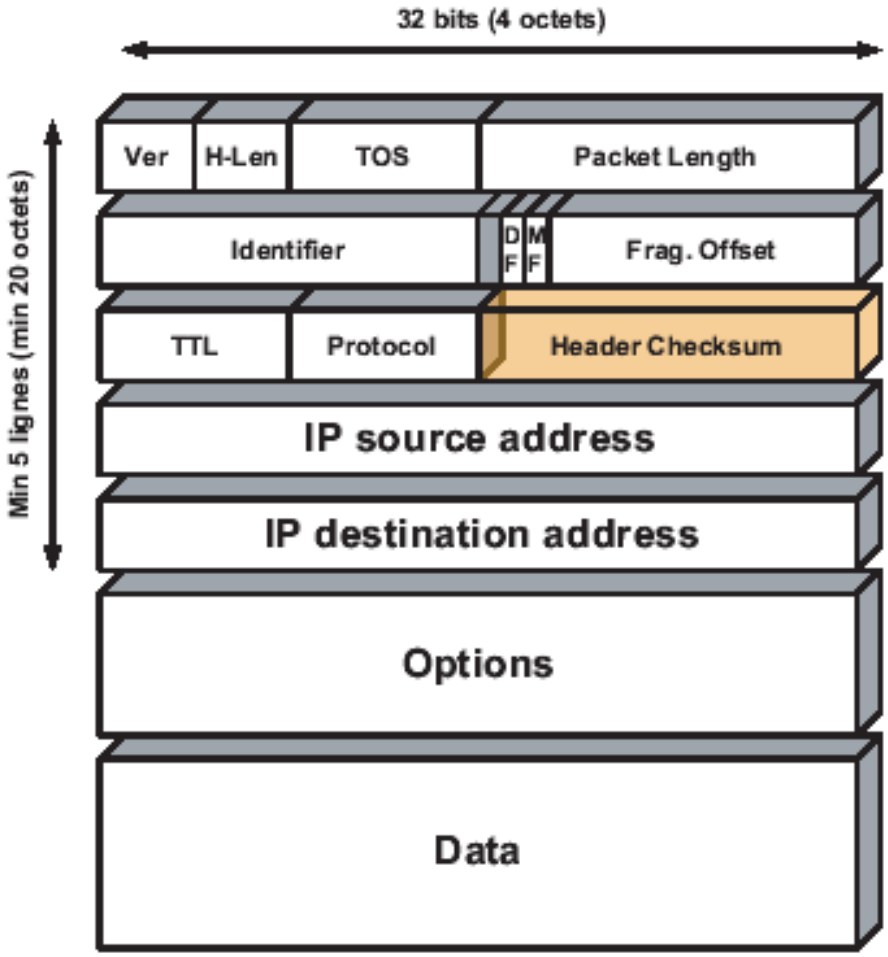
- démultiplexage vers les protocoles de la couches supérieurs
- 8 bits

Protocole transporté

```
Unix> cat /etc/protocols
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ce fichier contient les protocoles Internet tels qu'ils sont définis
# dans le document officiel RFC 1700 (Assigned Numbers).
#
# Format:
#
# <nom de protocole> <numro assign> [alias...]   [#<commentaire>]

ip          0       IP          # Protocole Internet
icmp        1       ICMP        # Protocole Internet de contrle de message
ggp         3       GGP         # Protocole passerelle-passerelle
tcp         6       TCP         # Protocole de contrôle de transmission ⇐
egp         8       EGP         # Protocole de passerelle externe
pup        12       PUP         # Protocole de paquet universel PARC
udp        17       UDP         # Protocole de datagramme utilisateur ⇐
hmp        20       HMP         # Protocole de surveillance d'hôte
xns-idp    22       XNS-IDP     # IDP Xerox NS
rdp        27       RDP         # Protocole de "datagramme fiable"
rvd        66       RVD         # Disque virtuel distant MIT
```

Le datagramme IP : champ Checksum

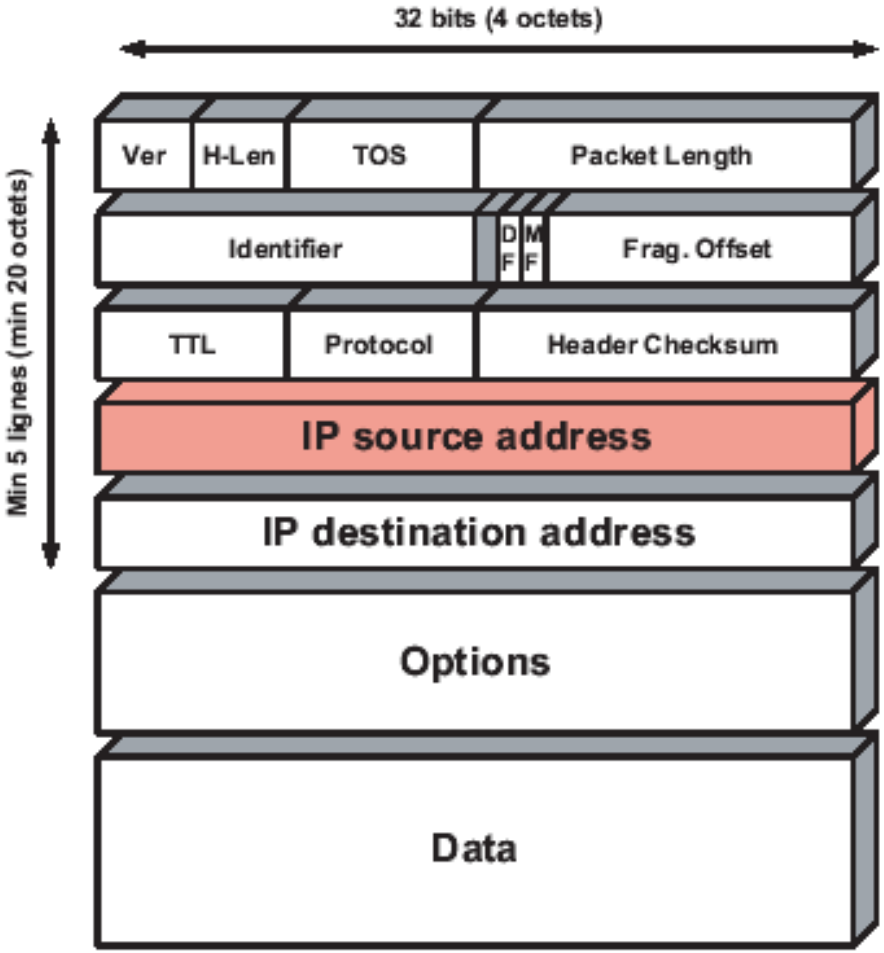


- 16 bits
- contrôle d'erreur sur l'entête
- aucun contrôle d'erreur sur le contenu
- vérifie si le paquet a été bien traité

$$\overline{\sum^{\overline{1}} mot_{16bits}}$$

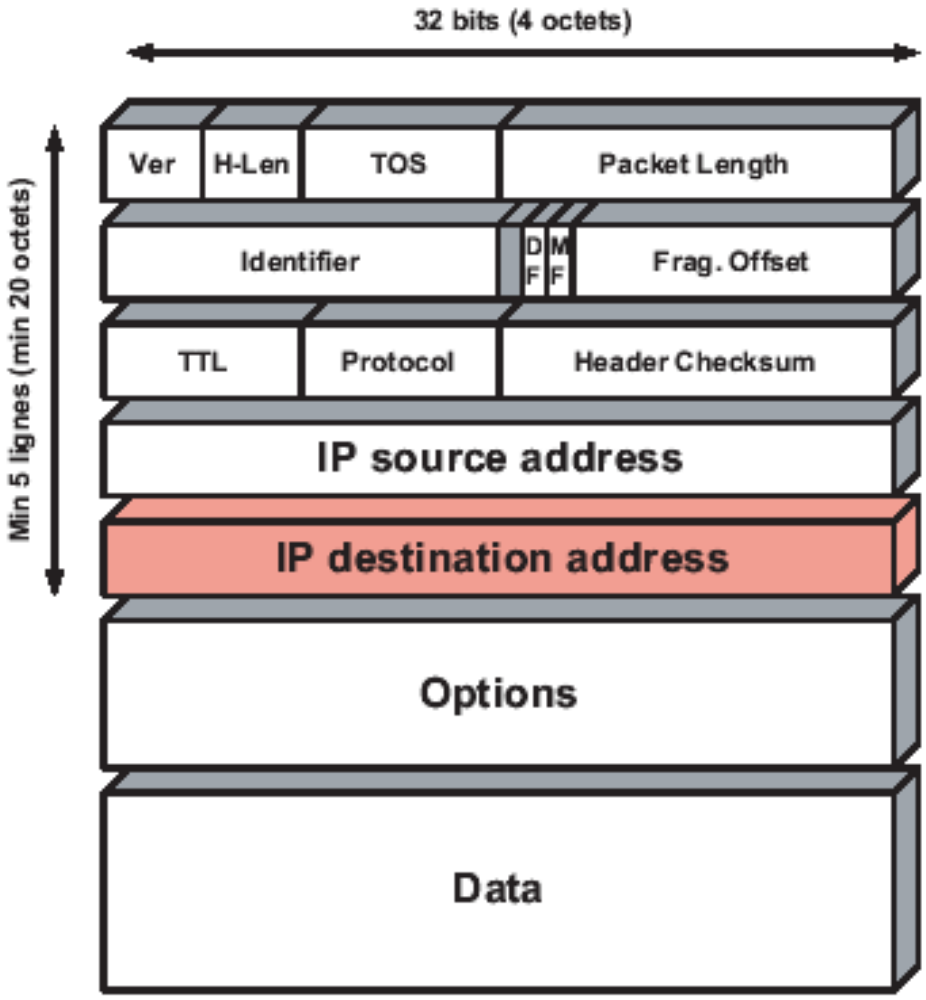
- recalculé à la sortie de chaque routeur
- si **faux** $\Rightarrow$ **paquet détruit**

Le datagramme IP : champ IP Source



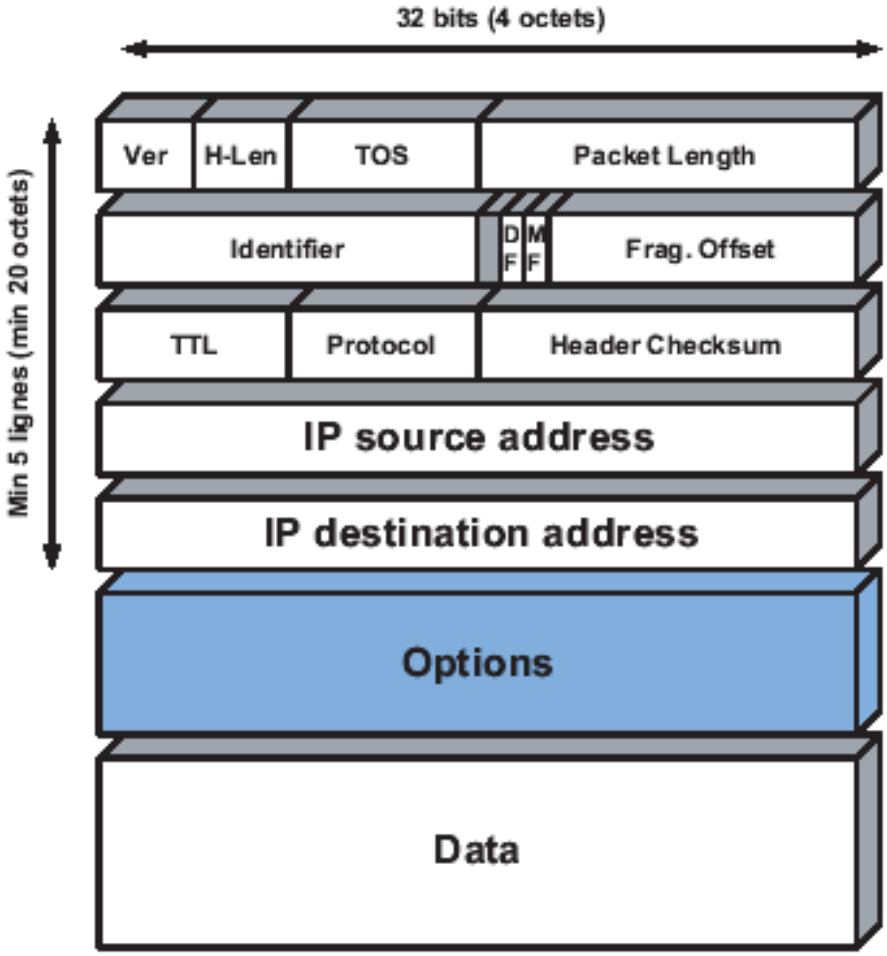
- adresse IP 32 bits
- identifie l'émetteur du paquet
- permet de retourner un message à l'émetteur (ICMP, UDP, ...)

Le datagramme IP : champ IP Destination



- adresse IP 32 bits
- indique le réseau du destinataire
- identifie l'interface du destinataire dans le réseau

Le datagramme IP : champ Options



- système TLV identique à TCP
- analysées dans chaque routeur
- 0 à 40 octets (alignés sur 32 bits)

Le datagramme IP : champ Options

Extension possible de l'entête IP

- Strict source route option
  - Permet à la source de spécifier la liste de tous les routeurs à utiliser pour attendre la destination
- Loose source route option
  - Permet à la source de spécifier la liste de certains routeurs intermédiaires à utiliser pour atteindre la destination
- Record route option
  - Permet de demander à chaque routeur traversé par un paquet d'insérer son adresse dans les options
- Router alert
  - Permet d'indiquer aux routeurs intermédiaires qu'ils doivent faire attention en traitant ce paquet

Contraintes : maximum 60 octets pour entête + option

Le datagramme IP : champ Options

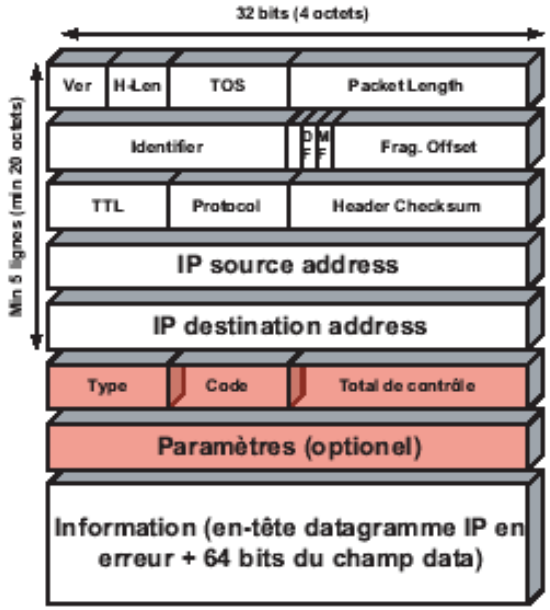
- La longueur indique la taille complète de l'option en octets.
- La liste complète des options est dans :
  - www.iana.org/assignments/ip-parameters
- Quelques options possibles sont :

Type (déc.)	Option	Objet
0	End of Options List (EOOL)	Utilisée si la fin des options ne coïncide pas avec la fin de l'en-tête.
1	No Operation (NOP)	Pour aligner le début de l'option suivante sur 32 bits.
130	Security (SEC)	Permet aux hôtes d'indiquer des restrictions liées à la sécurité (ex : non classifié, confidentiel, restreint, top secret, …).
131	Loose Source Route (LSR)	Permet à la source du datagramme de fournir des informations à utiliser par les passerelles pour le routage du datagramme vers sa destination et d'enregistrer l'information concernant la route (série d'adresses Internet) ; un routeur ou une route peut utiliser n'importe quelle route avec un nombre quelconque de passerelles intermédiaires pour atteindre la prochaine adresse indiquée dans la route.
68	Time Stamp (TS)	Enregistrement de l'heure de chaque passage de passerelle.
133	Extended Security (E-SEC)	
7	Record Route (RR)	Permet d'enregistrer la route d'un datagramme (en fait, l'adresse de chaque passerelle traversée).
136	Stream ID (SID)	Permet de véhiculer un identifieur de flux ; utilisée à des fins de débogage et de mesure.
137	Strict Source Route (SSR)	Idem LSR, si ce n'est qu'un routeur ou un hôte doit envoyer directement le datagramme à la prochaine adresse indiquée dans la route.

ICMP : Internet Control Message Protocol

ICMP – Internet Control Message Protocol

- Protocole de messages de contrôle de l'Internet
  - échange de messages entre routeurs : signaler une erreur réseau, demande d'information d'état, tests...
  - utilisé par des utilitaires (**ping**, **traceroute**, **NTP**)
  - permet de palier le manque de service de IP



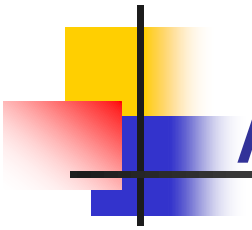
le champ Type :

- 0 : réponse Echo
- 3 : destination inconue
- 4 : limitation du débit par la source
- 8 : demande d'Echo
- 11 : expiration de délai (TTL=0)
- 12 : en-tête IP invalide
- 13/14 : requête/réponse d'horodatage

ICMP : Internet Control Message Protocol

ICMP – Internet Control Message Protocol

- `réponse/demande d'Echo` : utilisé par le ping
- `réponse/demande d'horodate` : idem mais heures incluses pour mesures de performances (utilisé pour NTP)
- `destination inconnue` : un routeur ne parvient pas à localiser la destination, problème de fragmentation (bit DF=1)
- `délai expiré` : paquet éliminé car le TTL a atteint 0 (boucle, congestion)
- `en-tête IP invalide` : la valeur d'un champ IP a une valeur illégale
- `ralentissement de la source` : contrôle de congestion, mais quasiment plus utilisé car génère du trafic supplémentaire (redondance car TCP gère la congestion)
- autres message
  http://www.iana.org/assignments/icmp-parameters

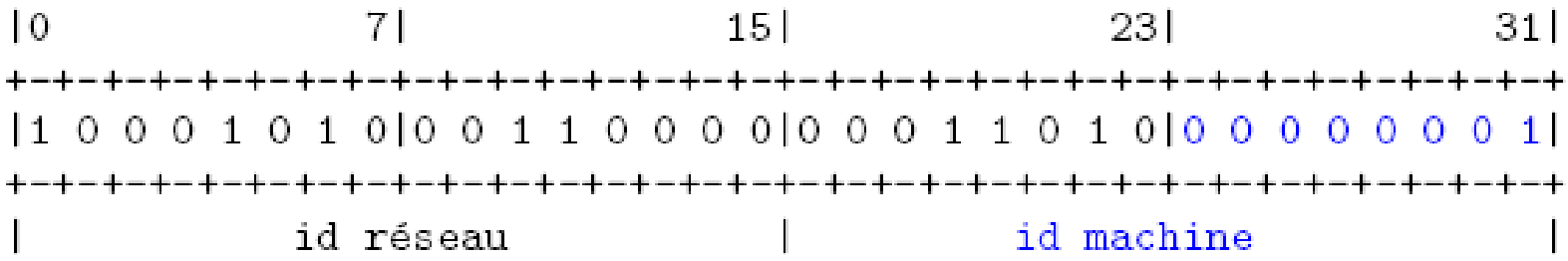


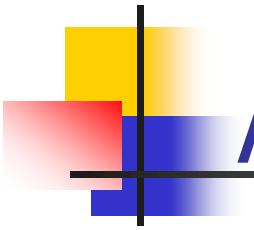
Adressage IP

- Adresse IP :
  - identificateur sur 32 bits
  - identifie une interface sur un hôte ou un routeur
- Interface : est le point d'accès de la station/routeur à la couche liaison de données (ex. carte Ethernet)
  - Une adresse IP est associée à une interface
  - Les routeurs ont typiquement plusieurs interfaces
  - Les hôtes peuvent avoir plusieurs interfaces, généralement il a une
- Exemples
  - www.yahoo.fr : 217.12.3.11
  - www.google.fr : 216.239.59.147

Adressage IP

- Structure d'une adresse IP
  - Une adresse IP, sur 32 bits, par interface sur chaque machine
  - Représentée par 4 valeurs décimales [0–255] séparées par des "." (codage réparti en 4 octets)
- L'adresse IP est divisée en deux parties, la partie id réseau et la partie id machine



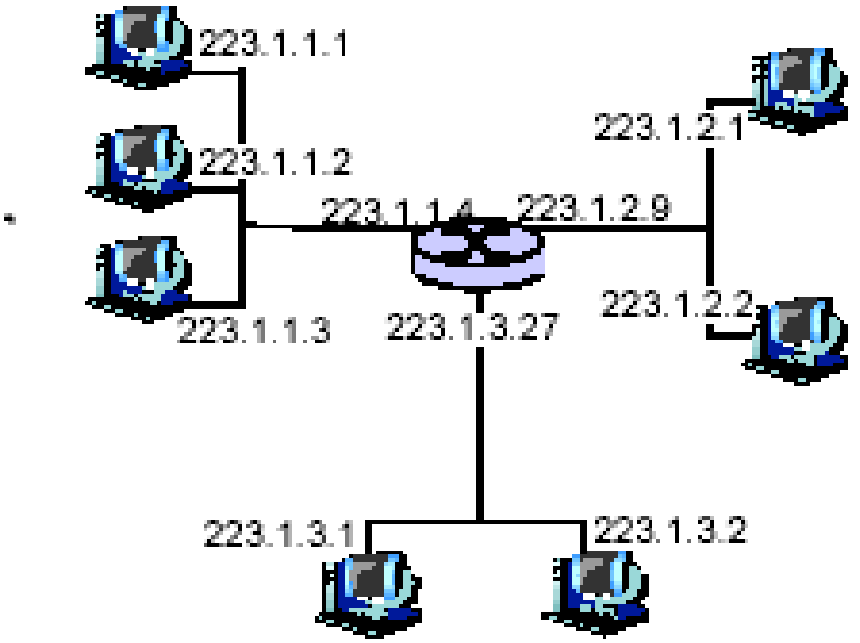


Adressage IP

- La partie ID_Réseau représente la partie réseau, partie qui sera commune à toutes les adresses IP d'un même réseau.
- La partie ID_Machine représente la partie hôte, c'est-à-dire la machine et sera unique sur un réseau.
- Le masque est nécessaire au calcul de réseau, car sans masque il est très difficile de savoir à quel réseau appartient une adresse.

Adressage IP

- Adresse IP
  - Partie réseau (bits de poids forts)
  - Partie hôte (bits de poids faible)

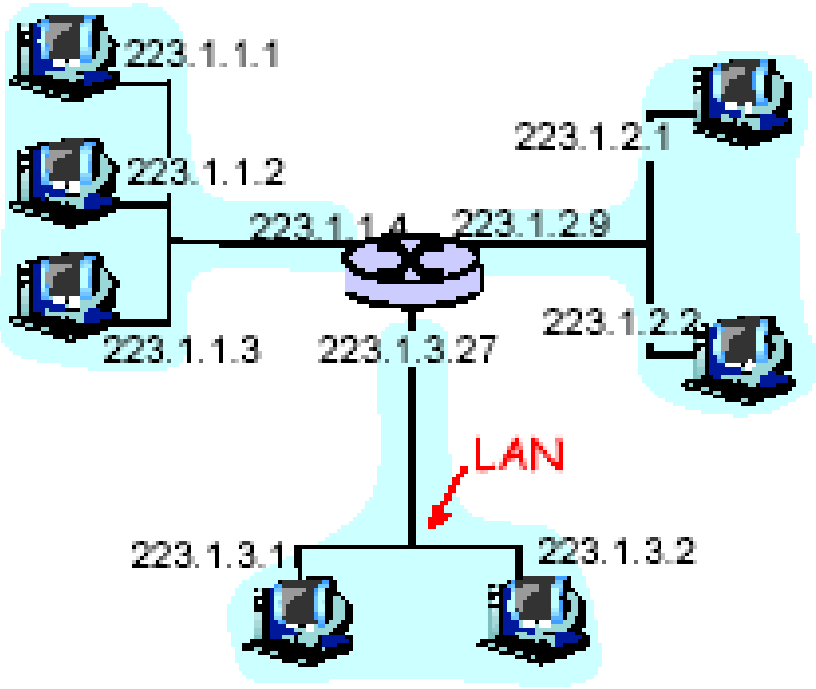


223.1.1.1 = 11011111 00000001 00000001 00000001

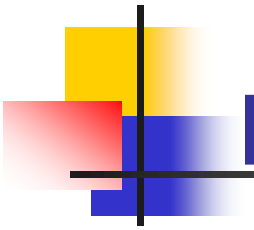
223 1 1 1

Adressage IP

- Réseau ? (du point de vue IP)
  - Les interfaces avec la même partie réseau de l'adresse IP
  - Et qui peuvent communiquer sans avoir besoin d'un routeur ou passerelle

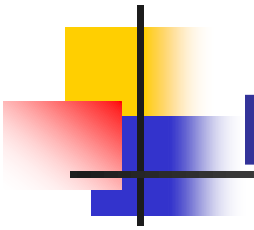


Le réseau est constitué de 3 réseaux IP (Les 24 premiers bits sont l'adresse réseau)



Pourquoi un subnet ?

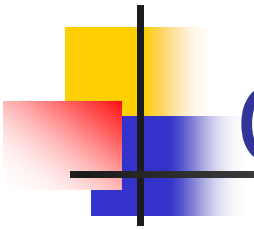
- Dans un réseau local Ethernet TCP/IP
  - problèmes de charge de réseau liés à une :
    - diffusion trop importante (broadcast)
    - trop grande quantité de machines sur un seul réseau logique d'ou un trafic trop important
- Dans un réseau local, MAN ou WAN par sécurité, on peut vouloir isoler certains utilisateurs de certaines ressources.
- Dans tout ces cas, tout en gardant les mêmes adresses TCP/IP, le découpage en sous-réseaux (subnetting)
  - associé à l'utilisation de routeurs



Pourquoi un subnet ?

- L'utilisation de TCP/IP oblige traditionnellement à choisir une classe d'adresse

- Chaque classe proposée offre un compromis entre le nombre maximum de réseaux et le nombre de machines



Quelles adresses TCP/IP utiliser ?

- Classes d'adresses
- Adresses spéciales
- Le masque de réseaux

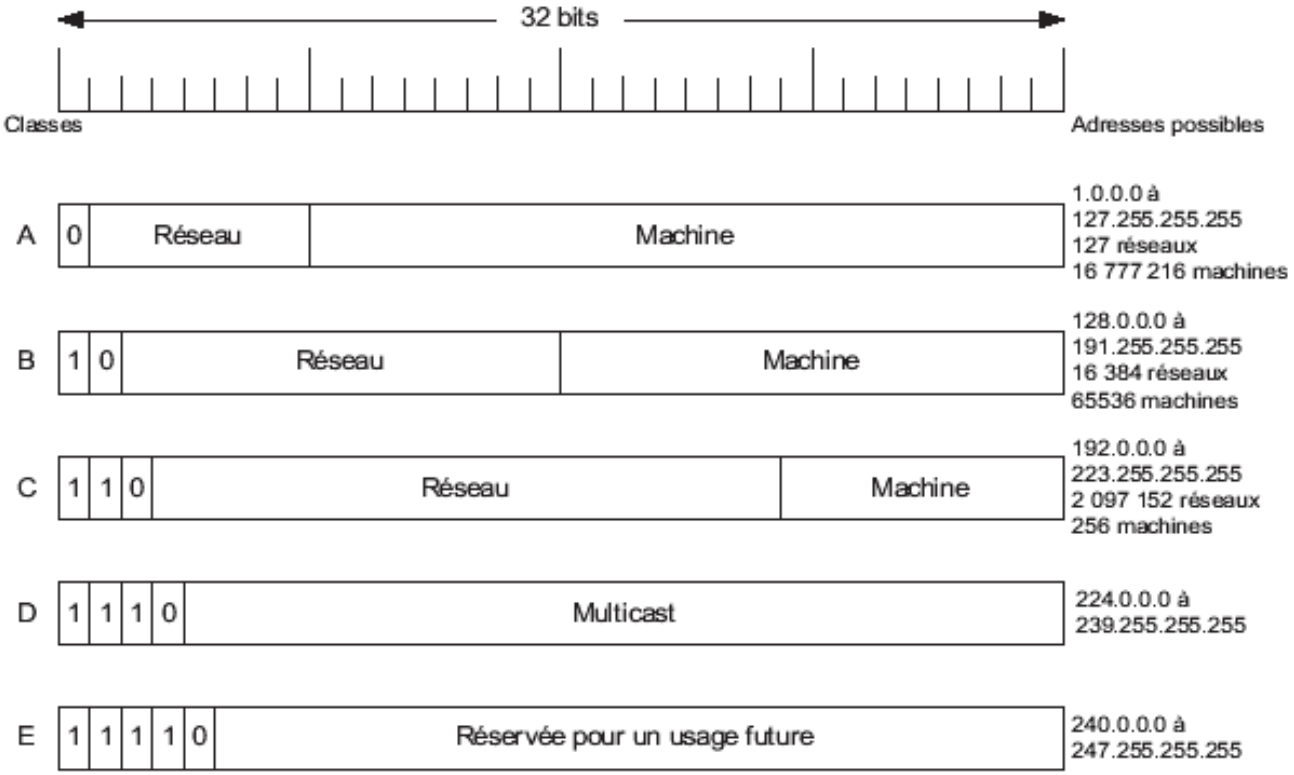
Les classes d'adresses

- Il existe à ce jour 5 classes d'adresses possibles :
  - plus le nombre de réseaux par classe est important, moins le nombre possible de machines est important

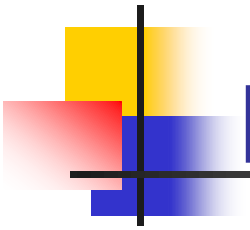
Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

- classe D : réservées au muticasting
- classe E : réservées à un usage futur (...)
- Les seules classes vraiment utiles pour le sous-réseaux sont les classes A, B et C

Les classes d'adresses

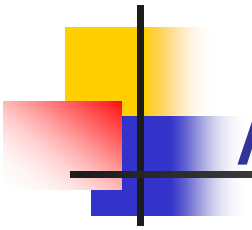


Les adresses réseaux sont distribuées par un organisme international à but non lucratif : **ICANN** (*Internet Corporation for Assigned Names ans Numbers*) puis décentralisé au niveau de chaque pays



Les classes d'adresses

- On peut alors choisir, à partir du nombre de machines que l'on compte mettre en oeuvre, le type de classe le plus approprié.
- Pour trouver à quelle classe appartient une machine donnée, il suffit de repérer la valeur du premier octet de l'adresse TCP/IP.
  - L'adresse 174.23.2.45 est par exemple une adresse de classe B, car le premier octet, 174, est compris entre 128 et 191.
  - L'adresse 5.6.7.8 est une adresse de classe A



Adresses IP Spéciales

- Toutes les dernières adresses d'un réseau sont des adresses de broadcast
  - En général, elles se terminent par 255, mais pas obligatoirement si le masque n'est pas courant (par exemple : 192.168.0.255 ou 80.34.255.255).
- Toutes les adresses finissant par 0 sont des adresses représentant le réseau
  - par exemple : 192.168.0.0 ou 12.54.255.0

- Adresses privées définies dans la RFC1918 :
  - pour la classe A les adresses 10.x.x.x
  - pour la classe B les adresses 172.16.x.x à 172.31.x.x
  - pour la classe C les adresses 192.168.x.x

Adresses IP spéciales

127.0.0.1 (localhost)

- Adresse virtuelle accessible sur chaque machine
- Permet de contacter un serveur sur la machine locale

10.0.0.0/8, **172.16.0.0/12** et **192.168.0.0/16**

- Réservé pour les réseau privés (non connectés à Internet!)

218.0.0.0/8 - 223.0.0.0/8 et **240.0.0.0/8 - 255.0.0.0/8**

- réservé pour une utilisation future

224.0.0.0/8 - 239.0.0.0/8

- réservé pour les adresses IP multicast

255.255.255.255

- Broadcast ≪ général ≫ (pas en pratique)

Reste

- Adresses IP de stations connectées à l'Internet global

Le masque de réseau

- Un masque réseau TCP/IP
  - est un ensemble de 4 octets (32 bits)
  - qui permet de distinguer, dans une adresse TCP/IP, la partie réseau de la partie machine.

_____Réseau_____Machine
11111111.11111111.11111111.00000000

- Ce qui s'écrit en décimal 255.255.255.0

- La partie réseau est représentée par des bits à 1, et la partie machine par des bits à 0
- Le masque ne représente rien sans l'adresse IP à laquelle il est associé.
- Exemple : l'adresse de la machine est 184.23.3.67, avec un masque de 255.255.0.0
  - Cette machine appartient au réseau 184.23.0.0.

Le masque de réseau

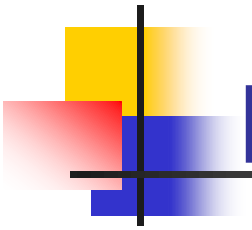
- Quelles adresses pour les masques ?
- Etant donné que l'on conserve la contiguïté des bits, on va toujours rencontrer les mêmes nombres pour les octets du masque. Ce sont les suivants:
  - 11111111
  - 11111110
  - 11111100
  - ...
  - 10000000
  - 00000000
- Soit en décimal : 255, 254, 252, 248, 240, 224, 192, 128, et 0.

- tous les masques possibles dans la RFC suivante :
- http://www.faqs.org/rfcs/rfc1878.html

Le masque de réseau

Quelle est cette notation avec un /, comme /24 ?

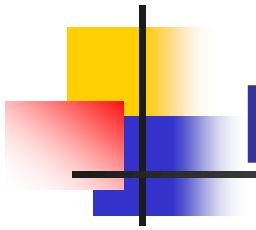
- Une autre notation est souvent utilisée pour représenter les masques
  - plus rapide à écrire
- Dans celle-ci, on note directement le nombre de bits significatifs en décimal, en considérant que la contiguïté est respectée.
  - Par exemple 192.168.25.0/255.255.255.0, on peut aussi écrire 192.168.25.0/24, car 24 bits sont significatifs de la partie réseau de l'adresse.
- De même, les écritures suivantes sont équivalentes:
  10.0.0.0/255.0.0.0 = 10.0.0.0/8
  192.168.25.32/255.255.255.248 = 192.168.25.32/29



Le masque de réseau

Rappel de fonctionnement :

- Quand un ordinateur cherche a communiquer avec un autre ordinateur ou avec un périphérique réseau quelconque en utilisant le protocole TCP/IP, la procédure suivante se déroule :
  1. Le nom de la machine est transformé en une adresse TCP/IP. Ceci est effectué par le resolver qui utilise un service de nommage (table hosts, DNS)..
  2. Les routines des couches TCP/IP associent ce numéro et le masque de réseau pour déterminer si la machine à atteindre fait ou non partie de même réseau.

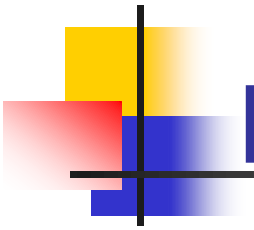


Le masque de réseau

2.1 Si oui, l'adresse TCP/IP est résolue en une adresse Ethernet; une trame est alors formée avec cette dernière et est envoyée sur le réseau.

2.2 Sinon, et si il existe une table de routage, l'adresse Ethernet du routeur est utilisée pour former une trame qui est envoyée sur le réseau (donc vers le routeur approprié).

3. Sinon, un message d'erreur est renvoyé vers le programme utilisateur (celui qui cherchait à envoyer des données). Ce message indique que l'adresse de la machine destinataire est impossible à joindre.



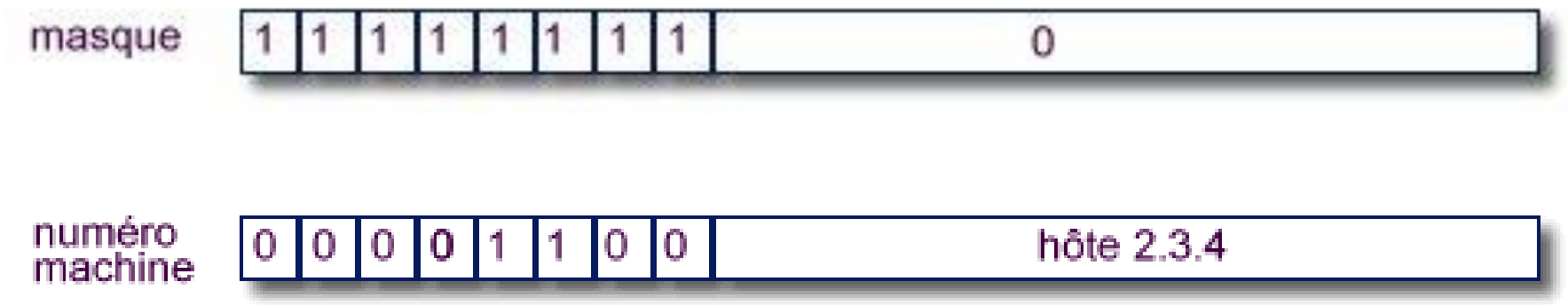
Le masque de réseau

Pour réaliser le masquage, on utilise l'opération AND binaire

- Masque sous-réseau = masque par défaut de la classe + bits utilisés pour le sous-réseau à 1
- Sous-réseau = adresse IP AND binaire masque de la classe (ou la masque du sous-réseau)
- Adresse de diffusion = Adresse du réseau + partie hôte avec tous les bits à 1
- Adresse machine = adresse IP AND binaire ~masque

Le masque de réseau

- Dans le cas d'une machine dont le numéro TCP/IP est 12.2.3.4 et le masque de 255.0.0.0, on a alors les valeurs de masque et d'adresse hôte ci-dessous :

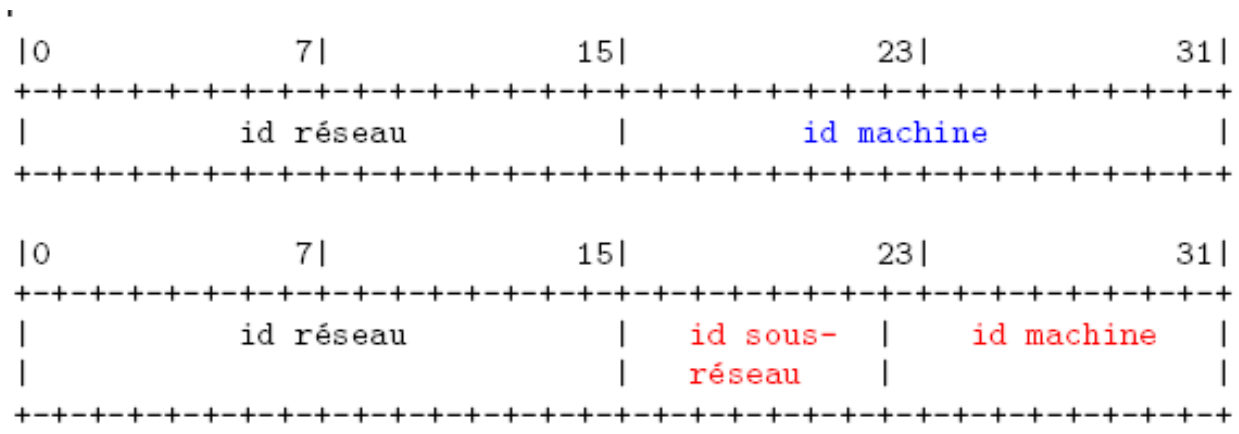


Création d'un sous-réseau

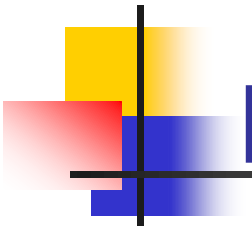
- Intérêt de diviser de grands réseaux en sous-réseaux
  - plus faciles à gérer
- l'espace d'adressage alloué doit être re-découpé
- Le (ou les) dernier(s) octet(s) va donc être utilisé pour "coder" un sous-réseau et une adresse de machine.
- Une contrainte va apparaître : chacun des sous-réseaux formé devra avoir une adresse de réseau et une adresse de diffusion (broadcast).
  - Ces deux adresses ne pourront pas être allouées à des machines.

Création d'un sous-réseau

- Comment diviser un réseau IP en plusieurs sous-réseaux IP ?
  - un troisième niveau de hiérarchie est mis en place (sous-réseau ou subnet)
  - prendre quelques bits de la partie id machine de l'adresse IP pour distinguer les sous-réseaux
  - transparent vis à vis de l'extérieur



Toutes les stations faisant partie d'un même sous réseau peuvent directement s'échanger des trames par l'intermédiaires de la couche liaison de données



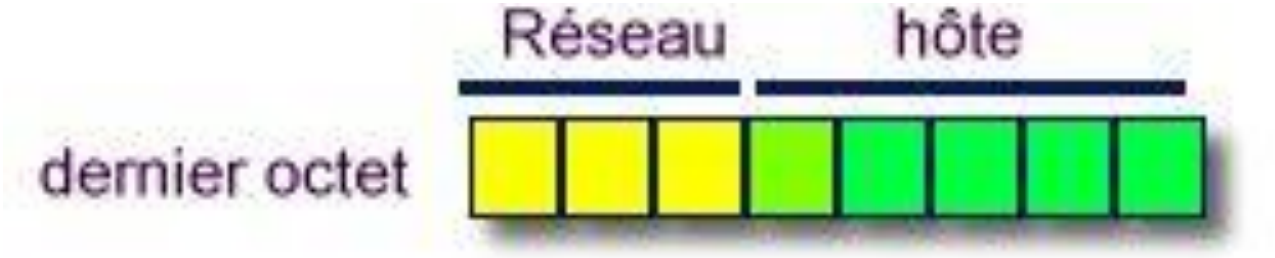
La création d'un sous-réseau

Exemple

- L'espace d'adressage 204.34.57.0 de classe C nous a été allouée avec un masque de 255.255.255.0
- Si on ne découpe pas en sous-réseaux, la totalité du dernier octet sert à numéroter les machines.
- Mais on désire créer des sous-réseaux :
  - on va donc re-découper l'espace fourni par les 8 bits du dernier octet.

La création d'un sous-réseau

- On peut par exemple allouer les bits de la façon suivante :



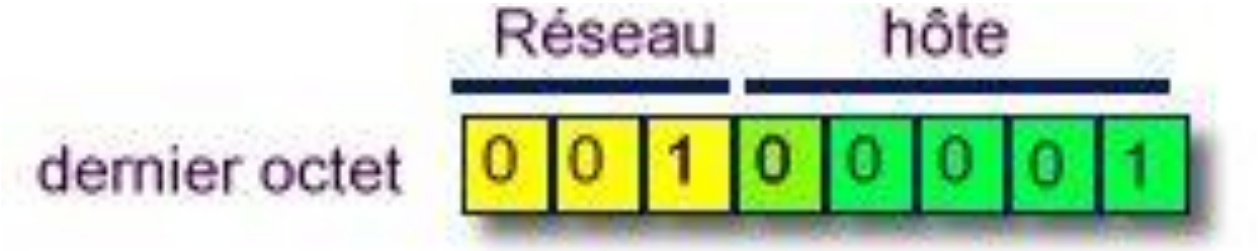
Les 3 bits de poids 32, 64 et 128 (jaunes) seront utilisés pour déterminer le sous-réseau et les 5 bits de poids 1, 2, 4, 8 et 16 (verts) pour définir les adresses des hôtes au sein des sous-réseaux.

La création d'un sous-réseau

- En groupant les bits de sous-réseau avec les bits de réseau, on va définir les sous réseaux suivants :
  - 204.34.57.0 (bits de sous-réseau = 000)
  - 204.34.57.32 (bits de sous réseau = 001)
  - 204.34.57.64 (bits de sous-réseau = 010)
  - 204.34.57.96 (bits de sous-réseau = 011)
  - 204.34.57.128 (bits de sous-réseau = 100)
  - 204.34.57.160 (bits de sous-réseau = 101)
  - 204.34.57.192 (bits de sous-réseau = 110)
  - 204.34.57.224 (bits de sous-réseau = 111)

La création d'un sous-réseau

- Pour notre exemple, on obtient donc 8 sous-réseaux possibles.
- Les bits de poids faibles (les bits verts) vont indiquer, pour chacun de ces sous-réseaux, les adresses à allouer aux machines.
- Par exemple, dans le réseau 204.34.57.32, la première machine portera l'adresse 1.
- Le dernier octet aura alors la valeur de 33



La création d'un sous-réseau

- Remarquez bien que l'on utilise les combinaisons 000 et 111 pour ces sous-réseaux.
  - La RFC950 qui stipulait que la première et la dernière adresse d'un réseau ne devaient pas être utilisées, est maintenant obsolète.

- En effet, la plupart des routeurs modernes savent très bien gérer des adresses réseau dont tous les bits de sous-réseau sont à 1 ou à 0.
- Pour plus de précision ➔ reportez-vous à la RFC1878 qui propose un découpage en sous-réseaux indépendant des classes (voir l'adressage CIDR - ip classless)

La création d'un sous-réseau

- L'adresse TCP/IP complète sera donc 204.34.57.33
- Ainsi de suite jusqu'à 204.34.57.62

- On ne peut utiliser l'adresse 204.34.57.63 pour une machine, car elle correspond a l'adresse de broadcast du sous-réseau 204.34.57.32

- Ensuite, dans le réseau 204.34.57.64, la première machine aura pour adresse 204.34.57.65 et ainsi de suite.

- En procédant ainsi, on a découpé un espace, où l'on pouvait initialement allouer 254 machines, en 8 sous-réseaux dans lesquels on ne peut allouer au total que 8 fois 30 machines.

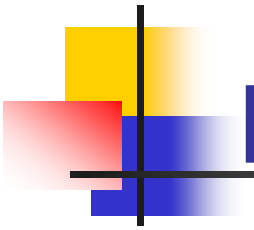
La création d'un sous-réseau

- Le tableau ci-dessous montre, en fonction des bits alloués soit au réseau soit aux hôtes, les différentes possibilités envisageables en classe C

bits réseau/ bits hôte	nb de sous - réseaux	nb d'hôtes	masque
1 / 7	2	126	255.255.255.128
2 / 6	4	62	255.255.255.192
3 / 5	8	30	255.255.255.224
4 / 4	16	14	255.255.255.240
5 / 3	32	6	255.255.255.248
6 / 2	64	2	255.255.255.252
7 / 1	128	0	255.255.255.254

Le masque du sous-réseau

- Avec ces nouveaux sous-réseaux, on doit également modifier le masque de réseau
- Pour notre exemple, le masque initial fourni pour la classe C était de 255.255.255.0
  - Mais on a utilisé les trois bits de poids fort du dernier octet pour coder les sous-réseaux
  - Il faut donc rajouter au masque initial le masque de sous-réseau. Ce dernier vaut 32+64+128, soit 224
- Le nouveau masque réseau est donc 255.255.255.0 + 224 = 255.255.255.224



Le masque du sous-réseau

- Pour résumer, le masque ne dépend que du nombre de bits affectés au réseau et au sous-réseau :
  - il suffit de positionner ces bits à 1 et de faire une somme binaire (un *OU binaire*) pour obtenir le masque
- Ce masque de réseau est important, car il va déterminer l'adresse de diffusion (broadcast) et, limiter les diffusions aux seules machines faisant partie d'un sous-réseau déterminé

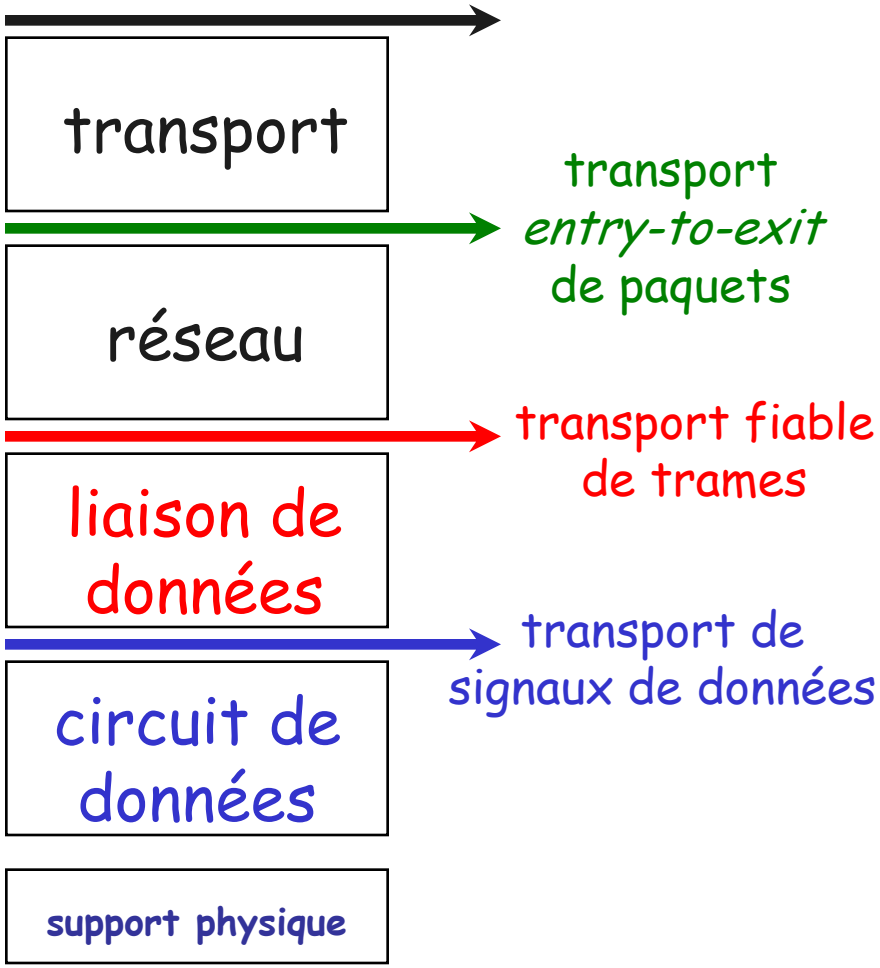
Les adresses de diffusion

- Chaque sous-réseau ainsi constitué doit avoir une adresse réseau, un masque de réseau et une adresse de diffusion (broadcast)
- L'adresse de diffusion est simple à calculer : elle correspond à l'adresse du réseau ou du sous-réseau plus l'adresse de l'hôte dont tous les bits sont à 1
  - Chaque sous-réseau possède une adresse de diffusion propre
  - Dans le cas du sous-réseau 204.34.57.32 (exemple traité), le numéro d'hôte dont tous les bits (les bits verts de la figure) sont à 1 est 31
  - Si on ajoute ce nombre à l'adresse du réseau, on obtient 204.34.57.32 + 31 = 204.34.57.63

Exemple 2 : sous-réseau classe B

bits réseau/ bits hôte	nb de sous - réseaux	nb d'hôtes	masque
1 / 15	2	32766	255.255.128.0
2 / 1 4	4	16382	255.255.192.0
3 / 13	8	8190	255.255.224.0
4 / 12	16	4094	255.255.240.0
5 / 11	32	2046	255.255.248.0
6 / 10	64	1022	255.255.252.0
7 / 9	128	510	255.255.254.0
8 / 8	255	254	255.255.255.0

Etat de notre architecture

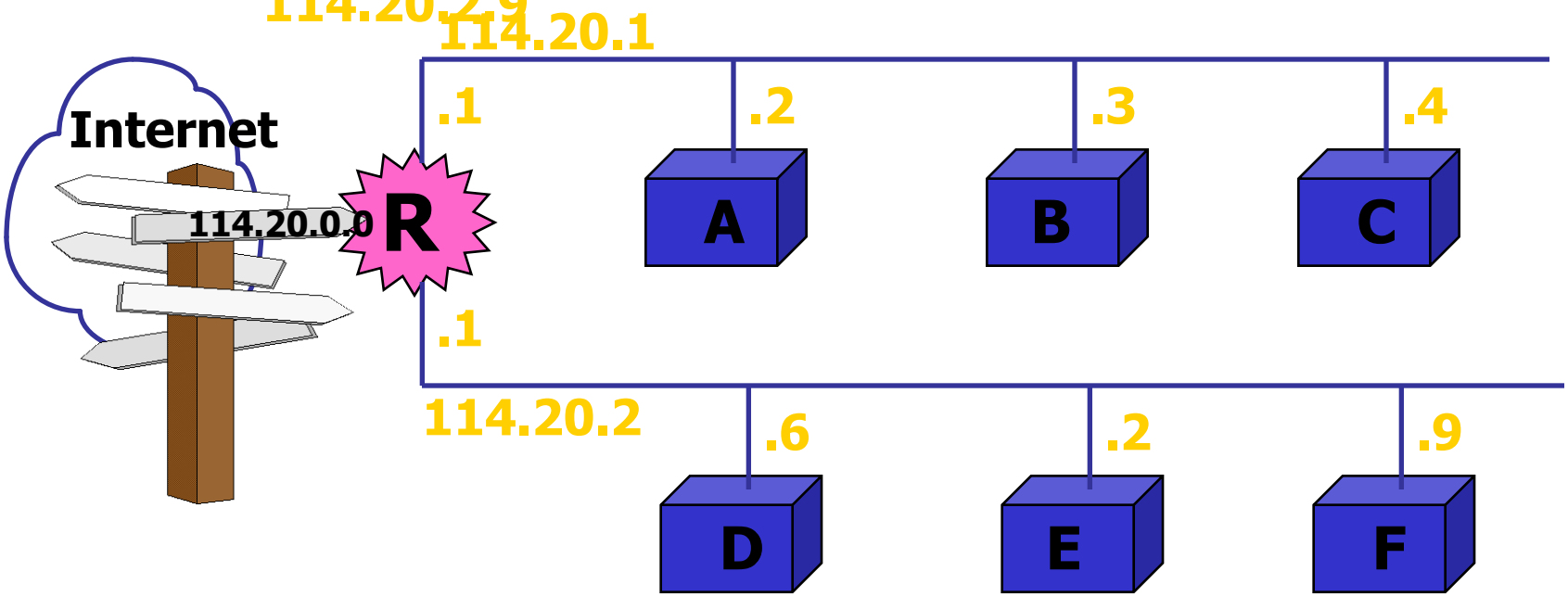


Exemple

UNIVERSITÉ PARIS DESCARTES

Les sous-réseaux 114.20.1.0 et 114.20.2.0 sont notés seulement avec le NetId, les machines seulement avec le Hostid.

exemple adresse IP de B = 114.20.1.3 et IP de F = 114.20.2.9



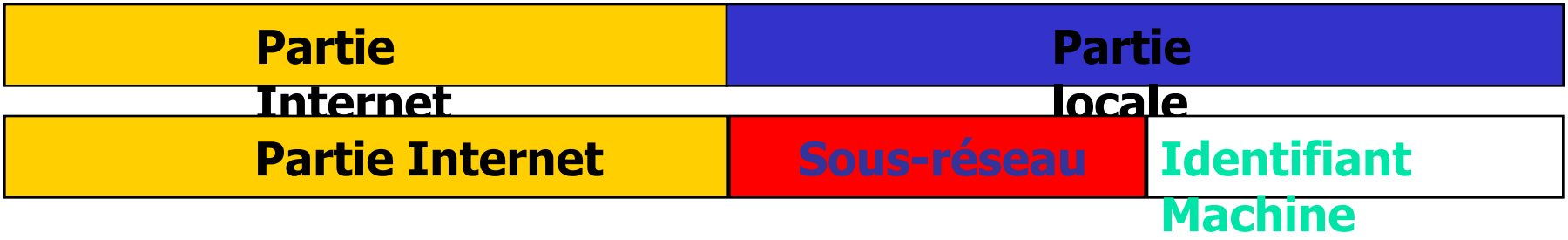
Le site utilise le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de classe B.
Le routeur R accepte tout le trafic destiné au réseau 114.20.0.0 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse destination.

Le fonctionnement (1)

- Le site utilise une seule adresse pour les deux réseaux physiques.
- A l'exception de R, tout routeur de l'internet route comme s'il n'existait qu'un seul réseau.
- Le routeur R doit router vers l'un ou l'autre des sous-réseaux ; le découpage du site en sous-réseaux a été effectué sur la base du troisième octet de l'adresse :
  - les adresses des machines du premier sous-réseau sont de la forme 114.20.1.x,
  - les adresses des machines du second sous-réseau sont de la forme 114.20.2.x.

Le fonctionnement (2)

- **«Partie Internet» correspond au Net-Id (plan d'adressage initial)**
- **«Partie locale» correspond au Host-Id (plan d'adressage initial)**
- **les champs «Sous-réseau» et «Identifiant Machine» sont de taille variable ; la longueur cumulée des deux champs est toujours égale à la longueur de la «Partie locale»**



UNIVERSITÉ
PARIS DESCARTES

Protocoles de contrôle de l'Internet et utilitaires réseaux

ICMP

ping et traceroute

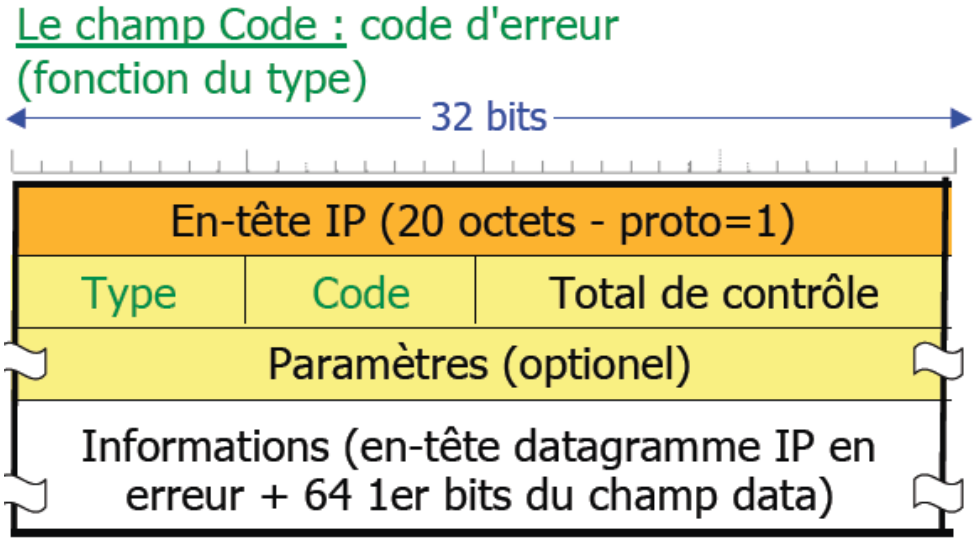
ARP et RARP

BOOTP et DHCP

Fichiers de config. et commandes UNIX

ICMP - Internet Control Message Protocol

- Protocole de messages de contrôle de l'Internet
  - échange de messages entre routeurs : signaler une erreur réseau, demande d'information d'état, tests
  - utilisé par des utilitaires (ping, traceroute, Network Time Protocol)



Le champ Type :
0 : réponse d'Echo
3 : destination inconnue
4 : limitation du débit par la source
5 : redirection (ICMP redirect)
8 : demande d'Echo
11 : expiration de délai (TTL=0)
12 : en-tête IP invalide
13/14 : requête/réponse d'horodatage
17/18 : requête/réponse de netmask

ICMP - Types de message

- réponse/demande d'Echo : utilisé par ping
- réponse/demande d'horodate : idem mais heures incluses pour mesures de performances
- destination inconnue : un routeur ne parvient pas à localiser la destination, problème de fragmentation (bit DF=1), …
- délai expiré : paquet éliminé car TTL a atteint 0 (boucle, congestion, …)
- en-tête IP invalide : la valeur d'un champ IP a une valeur illégale
- ICMP redirect : envoyé par un routeur à un noeud d'extrémité pour signaler une meilleure route (évite la mise à jour manuelle de toutes les tables de routage quand ajout d'un routeur…)
- ralentissement de la source : contrôle de congestion (mais quasiment plus utilisé car génère du trafic supplémentaire -> congestion au niveau TCP)
- autres messages : www.iana.org/assignments/icmp-parameters

L'utilitaire ping

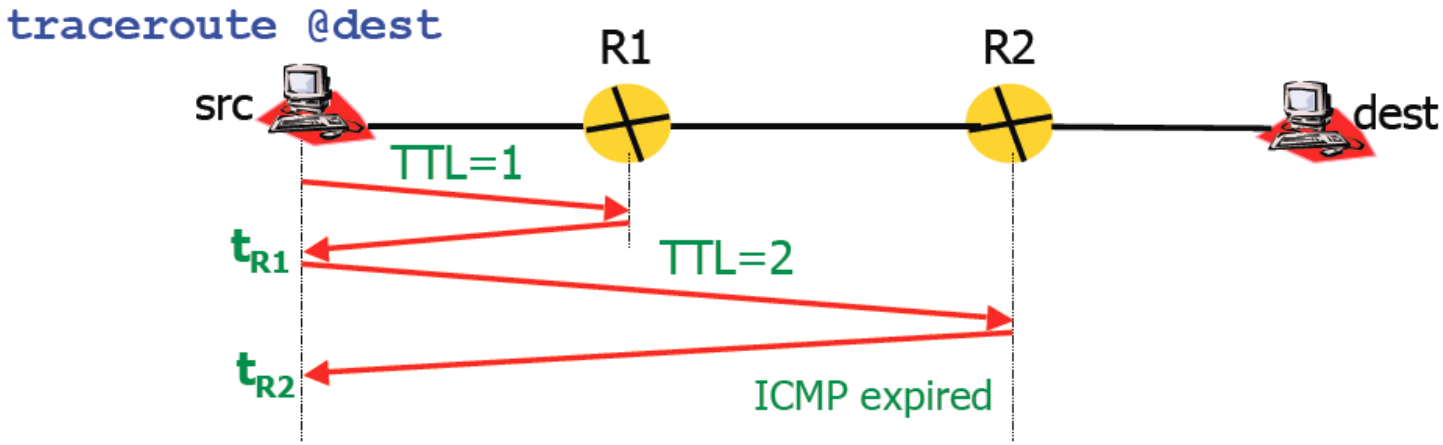
- **Ping : envoi d'un écho, attente de réponse, mesure du temps aller-retour**
  - teste l'accessibilité d'une destination **de bout en bout**
  - évaluation de performances
  - la réponse doit parvenir avant 20 secondes
- Exemples :
  - ping 127.0.0.1 : permet de tester la pile TCP/IP locale (en loopback)
  - ping mon@IP : permet de vérifier la configuration réseau locale de la station
  - ping @default-routeur : permet de tester la configuration du sous-réseau et de la passerelle
  - ping @dest : permet de tester un chemin de bout en bout

L'utilitaire ping

- **Ping : envoi d'un écho, attente de réponse, mesure du temps aller-retour**
  - teste l'accessibilité d'une destination **de bout en bout**
  - évaluation de performances
  - la réponse doit parvenir avant 20 secondes
- Exemples :
  - ping 127.0.0.1 : permet de tester la pile TCP/IP locale (en loopback)
  - ping mon@IP : permet de vérifier la configuration réseau locale de la station
  - ping @default-routeur : permet de tester la configuration du sous-réseau et de la passerelle
  - ping @dest : permet de tester un chemin de bout en bout

L'utilitaire traceroute (tracer sous windows)

- Permet de trouver pas à pas le chemin pour atteindre une destination
  - envoi d'un paquet IP avec TTL=1
  - attend ICMP délai expiré
  - envoi d'un paquet IP avec TTL=2, …

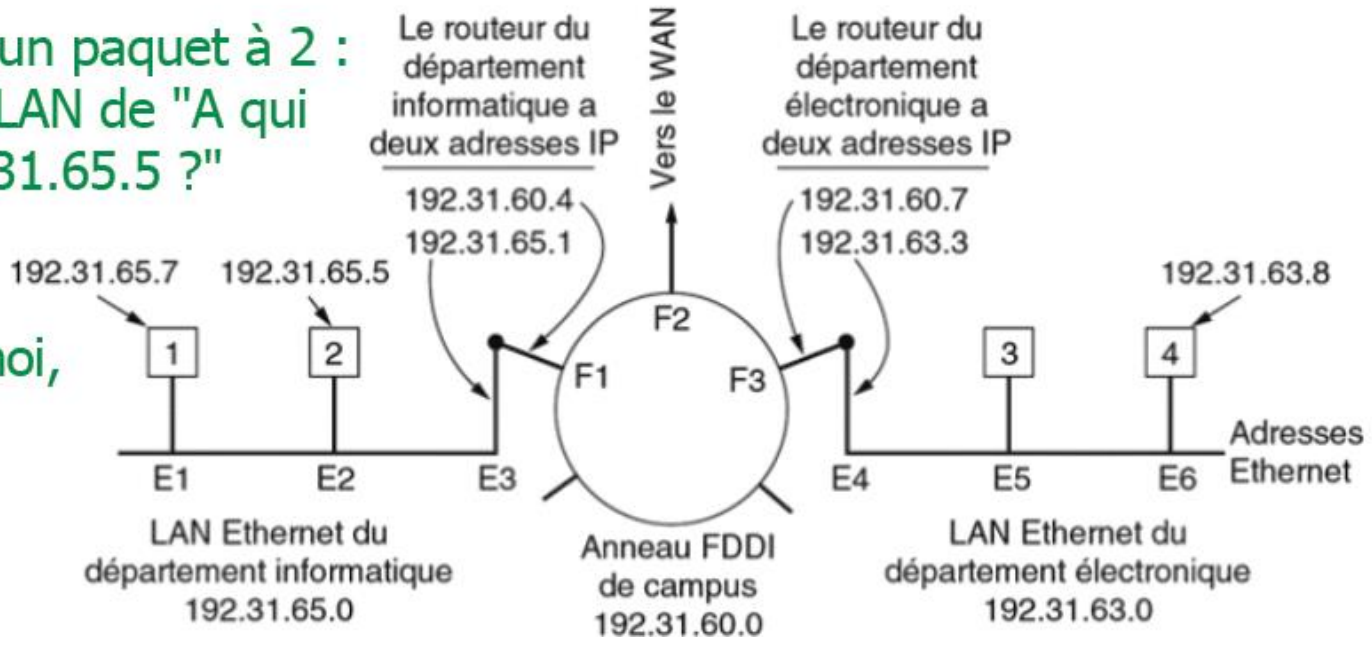


ARP - Address Resolution Protocol

- Problème : les équipements de liaison (cartes réseau…) ne comprennent pas les adresses IP mais utilisent des adresses physiques (MAC)
- Besoin d'associer @MAC <--> @IP

1 veut envoyer un paquet à 2 : diffusion sur le LAN de "A qui appartient 192.31.65.5 ?"

2 répond : "A moi, je suis E2"



ARP - Fonctionnement (1)

- Si la machine source et destinataire sont sur le même réseau (par ex. de 1 vers 2)
  - 1 - requête ARP (broadcast MAC)
  - 2 - réponse ARP (le destinataire a reçu le broadcast et s'est reconnu, il envoie son @MAC)
  - 3 - la source peut envoyer ses données vers le destinataire (adresse MAC destination connue)
- Si elles ne sont pas sur le même réseau (par ex. de 1 vers 4)
  - la diffusion ne passe pas le routeur
  - résolution de proche en proche : 1 envoie les données à 192.31.65.1 (ARP pour trouver E3), le routeur info envoie les données à 192.31.60.7 (ARP pour trouver F3), le routeur élec envoie les données à 4 (ARP pour E6)

ARP - Fonctionnement (2)

- Optimisations
  - Cache ARP : le résultat de chaque résolution est conservé localement pour les émissions suivantes
  - la correspondance **(@IP, @MAC)** de l'émetteur sont inclus dans la requête ARP pour que le récepteur, voire toutes les machines qui reçoivent le broadcast, mettent à jour leur cache

- Proxy ARP : une machine qui répond à une requête à la place du destinataire (qui ne reçoit pas le broadcast)
- nécessaire si la route (adresse de la passerelle) pour atteindre le destinataire n'est pas connue

RARP - Reverse ARP

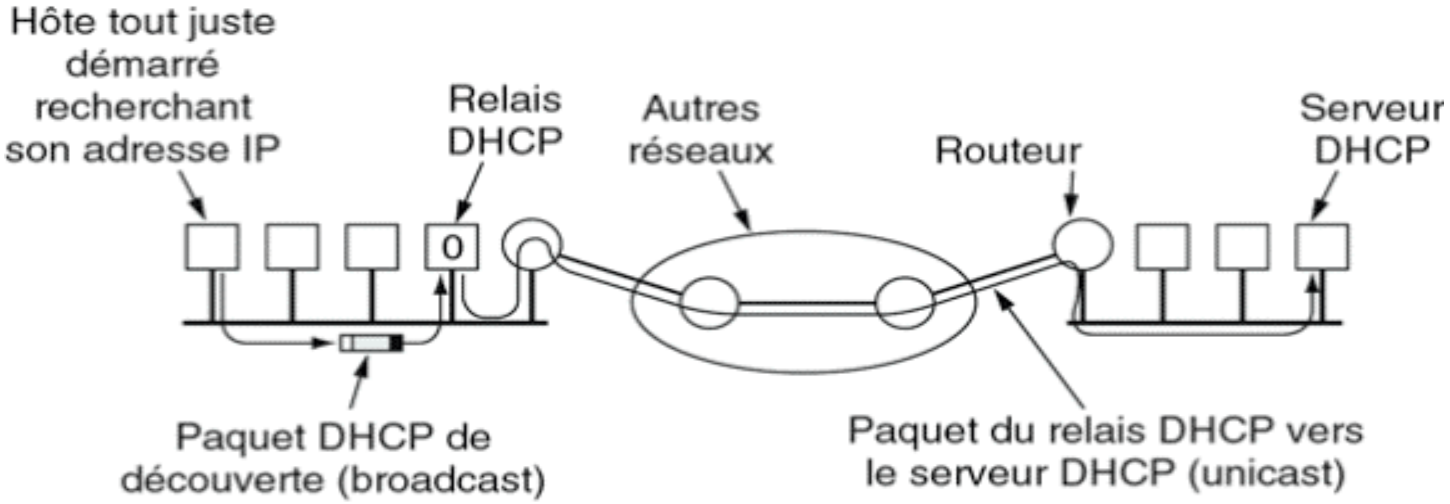
- ARP : @IP --> @MAC RARP : @MAC --> @IP
- "Mon @MAC est xx:xx:xx:xx:xx:xx. Quelqu'un connaît-il mon @IP ?«
- permet à un hôte de récupérer son @IP au démarrage par interrogation d'un serveur RARP
- stations sans disque
- imprimantes,…
- Même fonctionnement, même format de paquet
- Obsolète car désormais remplacé par BOOTP ou DHCP qui peuvent rendre le même service et ne nécessite pas un serveur RARP

BOOTP (bootstrap) - Principe

- Protocole d'amorçage du réseau au dessus de UDP (les diffusions passent les routeurs)
- le serveur informe la machine qui démarre de son @IP, @IP du serveur de fichiers qui contient son image disque, @IP du routeur par défaut, masque de sous-réseau
- Inconvénient : les tables de correspondances sont statiques (configurées manuellement)
- Pour y remédier, BOOTP est devenu DHCP : Dynamic Host Configuration Protocol

DHCP - Principe

- Configuration manuelle ou assignation dynamique des adresses IP
- Un serveur spécifique s'occupe d'assigner des configurations réseaux aux hôtes qui en font la demande
- Le serveur n'est pas nécessairement sur le même réseau (passage par un relais DHCP)



DHCP - Fonctionnement

- DHCP - économie d'adresses IP : quand un hôte quitte le réseau, il restitue son adresse
- Les messages DHCP (au dessus d'UDP)
  - **DHCPDiscover :** diffusion du client pour que les serveurs DHCP actifs répondent en fournissant une @IP
  - **DHCPOffer :** offre des serveurs (réponse à DHCPDiscover)
  - **DHCPRequest :** après avoir sélectionné une offre, le client émet une requête d'affectation d'@ au serveur élu
  - **DHCPAck :** le serveur renvoie une config. Réseau et une durée de validité (lease time)
  - **DHCPNAck :** refus d'un renouvellement par le serveur
  - **DHCPRelease :** résiliation du bail avant échéance par le client

Quelques fichiers de config sous LINUX/UNIX

- /etc/hosts : association locale nom/@IP
- /etc/resolv.conf : @ des serveurs de noms, noms de domaines
- /etc/protocols : association nom de protocole, numéro de protocole, liste d'alias
  - icmp 1 ICMP
  - tcp 6 TCP
- /etc/services : association nom de service, numéro de port/protocole, liste d'alias
  - ftp 21/tcp FTP
  - ssh 22/UDP
- /etc/inetd.conf : association entre nom de service et exécutable réalisant le service

Quelques commandes sous LINUX/UNIX

- ping : teste l'accessibilité d'une destination
- traceroute : renvoie la route prise par les paquets pour atteindre une destination
- arp : visualiser/modifier le cache ARP
- nslookup : interroger un serveur de noms
- netstat : obtenir des statistiques sur le nombre de paquets, les erreurs, les collisions, une interface, une table de routage, les sockets ouvertes, …
- tcpdump : visualiser des informations qui passent par l'interface réseau d'une machine

UNIVERSITÉ
PARIS DESCARTES

Protocoles de contrôle de l'Internet et utilitaires réseaux

Domaine Name System

D.N.S

Introduction (1/2)

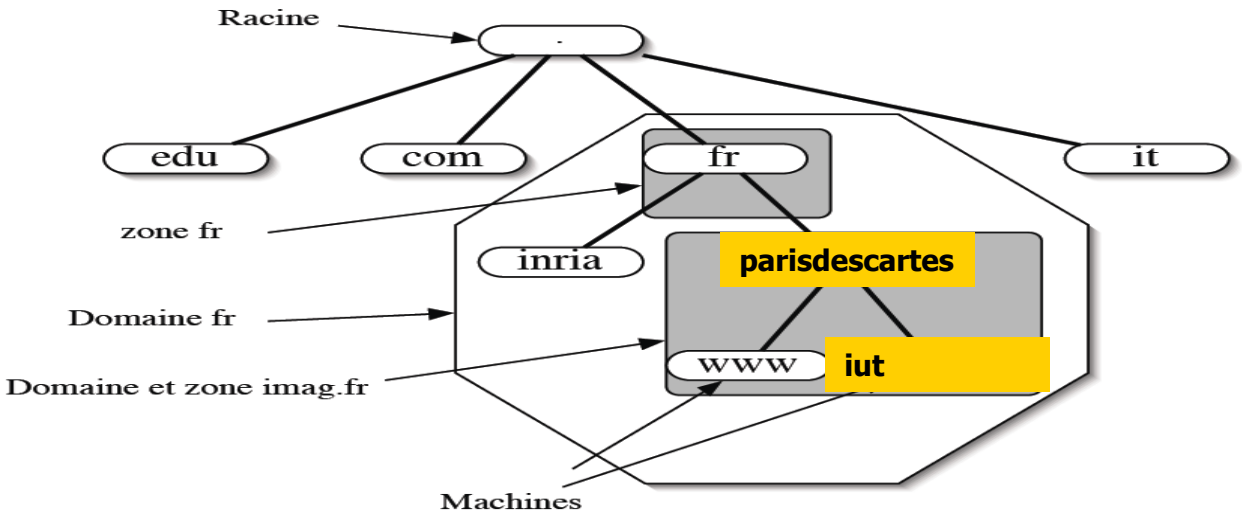
- Sur Internet une machine est identifié de manière unique par son adresse IP
- Annuaire Adresse IP / Nom
- Au début (1970-1984) : annuaire complet dans un fichier texte (/etc/hosts sous Unix):
  - – Adresse Nom1 Nom2 Nom3
  - – Cohérence des noms par diffusion du fichier
- Aujourd'hui ce fichier est encore utilisé pour l'annuaire local
- 1984 : mise en place du DNS
- Géré par Network Information Center (http://www.nic.com)
- En France Association Française pour le Nommage Internet enCoopération (http://www.afnic.fr)

Introduction (2/2)

- Information accessible grâce au DNS
  - Adresse en fonction du nom
  - Nom en fonction de l'adresse IP : résolution inverse
  - Adresse de relai de messagerie
- Système hiérarchique, redondant et distribué
  - Arborescence (comme un système de fichier)
  - Chaque site est maître de ses données
  - Dynamique: mise à jour automatique
- Documentation
  - http://www.dns.net/dnsrd (RFC, FAQ ...)
  - http://www.nic.f/guides
  - http://www.nic.fr/formation
- Bibliographie
  - DNS and BIND , Paul Albitz and Cricket Liu

Structuration des noms DNS

- Hiérarchique par domaine: www.parisdescartes.fr
  - machine www dans le domaine parisdescartes lui-même dans le domaine fr
  - Analogie nom de fichier/répertoire à l'envers avec le . à la place de /
  - On omet en général la racine (le point) : www.parisdescartes.fr.
  - Les majuscules ne sont pas significatives



Une base de données distribuée

- Une base de donnée est associée à chaque nœud
- L'ensemble de ces bases de données constitue le DNS
- Dans un noeud, on trouve
  - Les informations permettant de retrouver les noeuds fils
  - Les informations propre au noeud : liste des machines
  - Comme dans un répertoire : des sous répertoires et des fichiers
- La gestion de chaque noeud peut être effectuée par des entités différentes

Terminologie

- Domaine
  - Un domaine est la partie de l'arborescence à partir du noeud portant son nom
  - Exemple: domaine *fr:* *arborescence à partir du noeud* *fr*
  - On parle de sous domaine pour un domaine inclu dans un autre
  - Exemple: ***parisdescartes .fr*** *est un sous domaine du domaine* ***fr***
- Zone
  - C'est la base de donnée associée à un nœud
- Contenu des bases de donnée associées aux zones
  - Exemples: Noms/Adresses des serveurs de la zone
- Racine: liste des serveurs des domaines de premiers niveaux
- *fr: listes des adresses des serveurs des sous-domaines de fr*
  - Noms/Adresses des machines de ce domaine

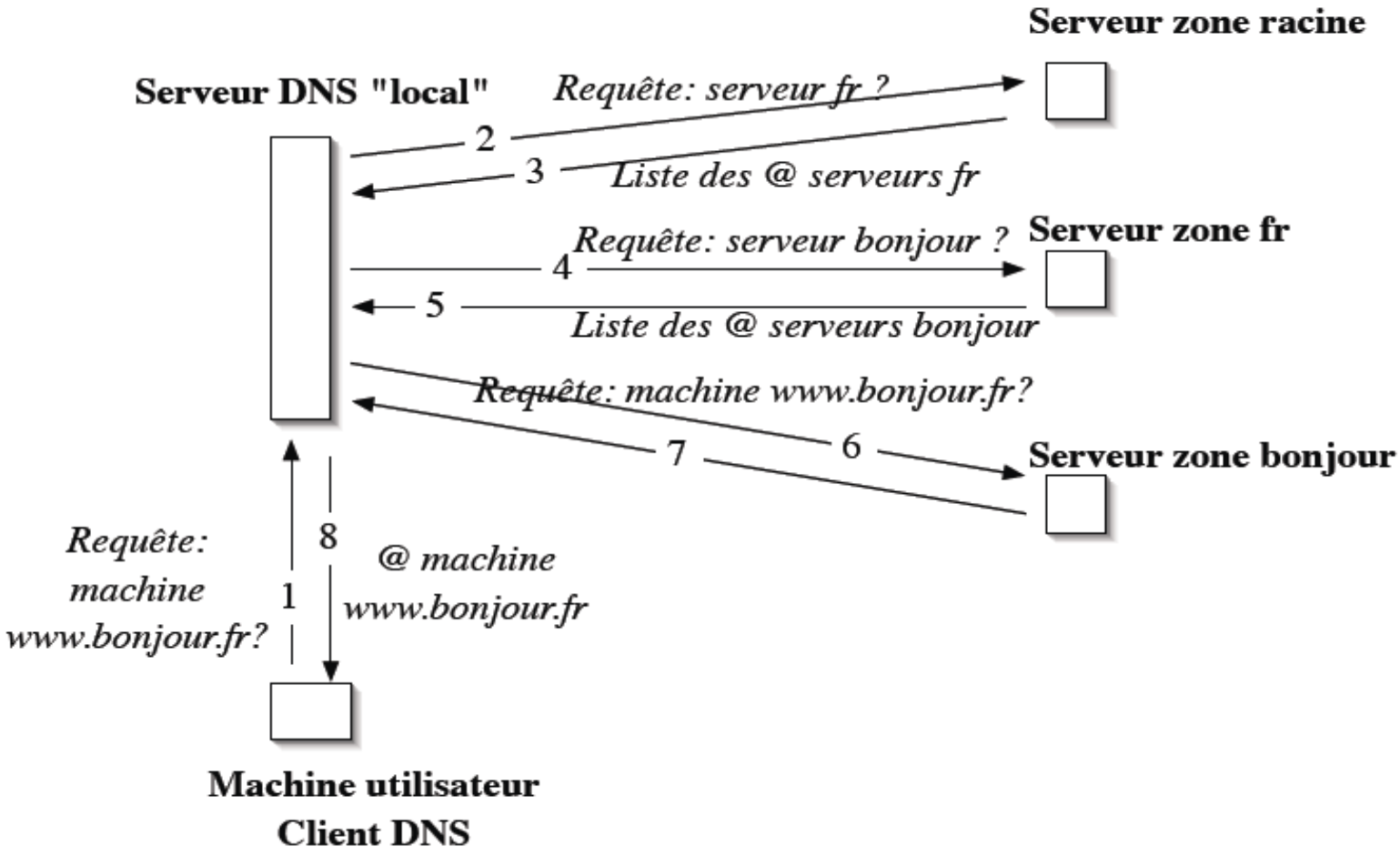
Domaines existants

- Terminologie de l'AFNIC: Domaine. Suffixe
- Suffixe ou Top Level Domain(TLD)
- Par pays (ou Country Code, ccTLD) en deux lettres :
  - Exemple : .fr, .us, .jp, .be
  - ICANN (Internet Corporation for Assigned Names and Number) : *http://www.icann.org/cctlds/*
  - IANA (Internet Assigned Numbers Autority) : *http://www.iana.org/cctld/cctld.htm*
  - Liste des contacts des différents ccTLD: *http://www.iana.org/cctld/cctld-whois.html*
- Génériques internationaux (gTLD) en trois lettres
  - .com (entreprise multinationale), .org (organisation), .edu (Université)
  - .net (fournisseur d'accès), .pro (profession libérale)
  - Liste des domaines génériques et de leur registre associé: *http://www.iana.org/gtld/gtld.htm*
  - Liste des nouveaux domaines(.aero, .biz, .coop, .info, .museum, .name, .pro) : *http://www.icann.org/tlds/*

Principe de fonctionnement

- Application client/serveur
- Serveurs DNS
- Gère la base de données contenant
- nom/@IP des machines du domaine
- nom/@IP des serveurs d'un sous-domaine
- Système robuste par redondance: plusieurs serveurs possèdent la base de donnée d'un domaine
- Client DNS
  - Resolver: permet l'interrogation d'un serveur
  - Référence à un serveur DNS par défaut "local"
- Interrogation client -> serveur local
  - Récursive
  - Le client attend la réponse finale
- Interrogations serveur-> serveur
  - Itératives

Exemple d'une interrogation DNS



Interrogation DNS

- Pour une zone : une liste d'adresse de serveurs
  - Répartition des interrogations
  - Requêtes successives si défaillance d'un serveur ou du réseau
  - Importance de la répartition géographique des serveurs d'une même zone
- Mécanisme de cache dans le serveur "local" pour limiter le nombre d'interrogations
  - Evite la surcharge du réseau
  - Diminue les délais de réponse
  - Baisse la charge des serveurs de haut niveau
- Remplissage du cache lors des requêtes des clients
- Durée de vie limitée dans le cache
  - TTL(Time Ti Live) spécifié dans les réponses

Serveurs

- Racine : environ 15 serveurs de nom répartis dans le monde
  - Connaissent tous les serveurs de premier niveau (TLD): .fr, .com, ...
  - Serveur origine (ou primaire, ou maitre) géré par IANA/ICANN
    - A.ROOT-SERVERS.NET
  - SERVEURS MIROIRS (ou secondaire, ou esclave)
    - de B.ROOT-SERVERS.NET à M.ROOT-SERVERS.NET
- Modification manuel faite sur le serveur primaire
- Échange des bases de données automatique vers les serveurs secondaires

Type de requêtes

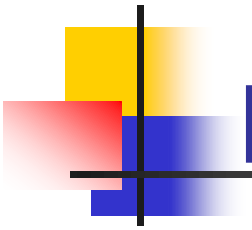
- Machines ?
  - Dénotée *a pour IPV4*
  - Possibilités de plusieurs machines pour un même nom
  - » Réponses “circulaires” pour répartir la charge
  - Dénotée aaa pour IPV6
- Plusieurs noms possibles pour une adresse IP
  - Un nom canonique: dénotée *cname*
- Serveurs d’une zone ?
  - Dénotée *ns*
- Relais de messagerie
  - Dénotée *mx*

Implémentation

- JEEVES :première implémentation du DNS (1984)
- BIND (The Berkeley Internet Name Domain) sur BSD Unix
- Interrogation en UDP ou TCP si la taille du paquets dépasse 512 octets
- Echange des bases de données en TCP
- Client
  - à travers les fonctions de programmation comme gethostbyname,
  - gethostbyaddr...
  - – outils associés
- • Serveur processus particulier
  - – Port 53 en TCP ou UDP
  - – nom: named

Outils DNS

- nslookup
  - *nslookup www.google.fr*
  - Changement de serveur : *server ns2.nic.fr*
  - mode debug: set debug
  - Serveurs d'une zone: *set q=ns*
  - Adresses pour un nom: *set q=a*
  - Serveurs de courrier: *set q=mx*
  - Nom canonique: *set q=cname*
  - Visualisation de la base de donnée: *ls imag.fr*
- host
  - Mode debug : *-d*
  - Type de requête: *-t a , -t ns …*
- dig

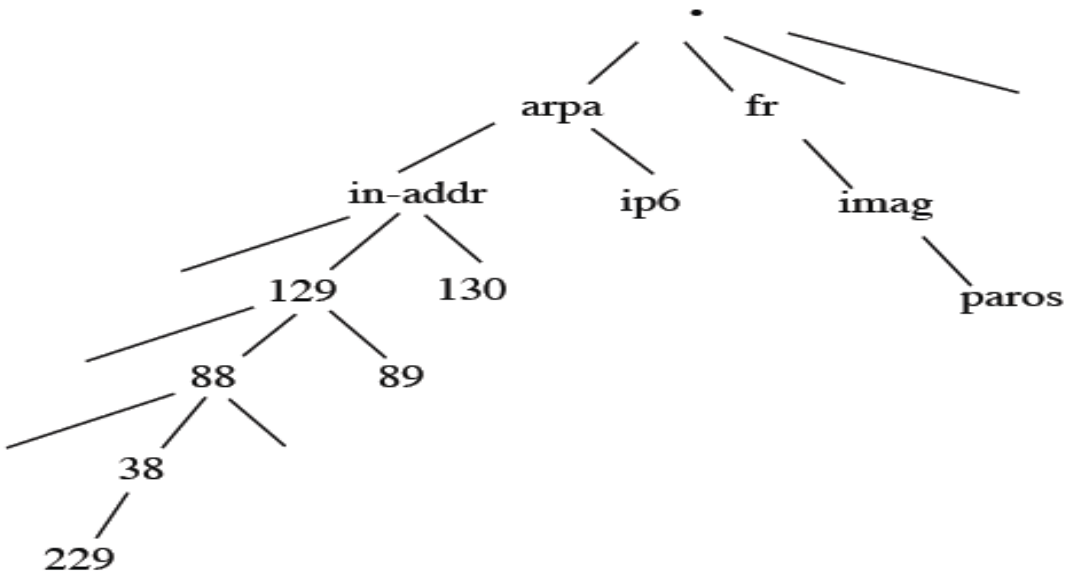


Résolution inverse

- Trouver le nom à partir de l'adresse
- Même principe que pour les noms
- Chaque octet de l'adresse IP est vue comme un sous domaine
- Un domaine TLD particulier : arpa
- Sous domaines
  - in-addr pour les adresses IPV4
  - ip6 pour les adresses IPV6
- Exemple: 229.38.88.129.in-addr.arpa

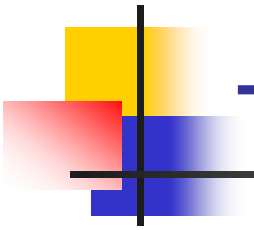
Exemple de résolution inverse

- paros.imag.fr
- 229.38.88.129.in-addr.arpa



Le DNS dans la pratique

- Le serveur
  - Fichiers de configuration
    Unix/linux: */etc/named.conf*
    Free BSD: */etc/namedb/named.conf*
  - Base de données
    Spécifié dans le fichier de configuration
  - Lancement du serveur
    Unix/linux: */etc/rc.d/init/named restart*
    Free BSD: *named -b /etc/namedb/named.conf*
- le client
  - – Fichier de spécification du serveur DNS: /etc/resolv.conf
  - – Fichier de spécification de la résolution de nom:
    Unix/linux: /etc/nsswitch.conf
    Free BSD: /etc/host.conf



TP

Analyse DNS

Lancez à l'aide d'un analyseur de protocoles une capture lors d'une demande de résolution de noms (suite à une demande de site web, à un ping, à un relevé de courrier…)

Quel est le protocole de niveau transport utilisé ? Justifiez.

Quel est le numéro de port de destination ? Justifiez.

Quelle est le type de requête DNS (le type de RR) ?

La requête est-elle de type récursive ? Quel est l'autre type de requête ?

Combien y-a-t-il de RR dans la réponse ? A quoi correspondent-ils ?