INTERNET : introduction et adressage

Plan

1. Introduction à L'INTERNET: Historique et définitions
2. Protocoles IP : Adressage
3. Protocole ARP : Résolution d'adresses
4. Protocole ICMP : contrôle des erreurs
5. Mode d'accès à Internet : ADSL, PPP

Bibliographie

- **TCP/IP : Principes, protocoles et Architecture**
  Douglas E .Comer, Prentice Hall - 4ème édition - 754 pages

- **TCP/IP Illustré vol. 1, 2 et 3**
  W. Richard Stevens, Addison-Wesley 1996

- **Routage dans l'Internet**
  Christian Huitema, Prentice Hall - 2ème édition - 384 pages

- **Réseaux locaux et Internet : Des protocoles à l'interconnexion**
  Laurent toutain, Hermès - 2 ème édition - 732 pages

Historique

- 1969 : Début du réseau (D)ARPANET (4 calculateurs)
- DARPA = Defense Advanced Research Projects Agency
- 1972 : Démonstration de ARPANET
  - IMP - Interface Message Processor - mode connecté (X.25)
  - NCP - Network Control Program – non connecté (ancêtre de TCP)
- 1977-1979 : Les protocoles TCP/IP prennent leur forme définitive,
- 1980 - L'université de Berkeley intègre TCP/IP dans Unix (BSD)
- 1980 - janvier 1983 : Tous les réseaux raccordés à ARPANET sont convertis à TCP/IP

Historique (2)

- 198x – TCPIP devient le Standard de facto pour l'interconnexion de réseaux hétérogènes,
- 1988 – Mise en place du Backbone de la NSFnet (12 réseaux régionaux)
- 1992 – EBone et RENATER
- 199x - explosion de l'offre et de la demande de services Internet y compris pour les particuliers
- 1995 – Arrêt du Backbone NSFnet
  - Mise en œuvre des NAPs (Network Access Points)
- 200x – Internet nouvelle génération

Qu'est ce qu'Internet ?

3 définitions

1. Une famille de protocoles de communication, appelée :
   - TCP / IP : Transmission Control Protocol / Internetworking Protocol,
   - ou Internet Protocol Suite,

2. Un réseau mondial constitué de milliers de réseaux hétérogènes, et interconnecté au moyen des protocoles TCP/IP :
   - Réseaux locaux d'agences gouvernementales, institutions d'éducation, hôpitaux, des commerciaux, …
   - Réseaux fédérateur de Campus,
   - Réseaux Régionaux, Nationaux, Intercontinentaux (Américains, Européen, Eunet, Ebone, Asiatiques, …)

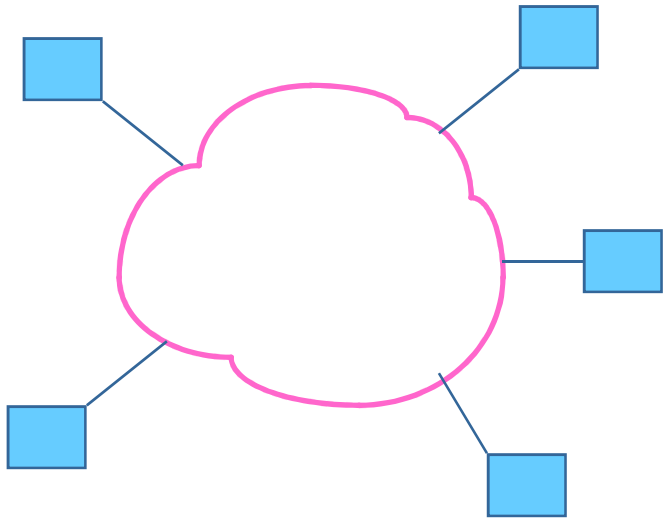
3. Une communauté de personnes utilisant différents services
   - Courrier électronique, Web, Transfert de fichiers FTP, …

Qu'est ce qu'un Intranet ou Extranet ?

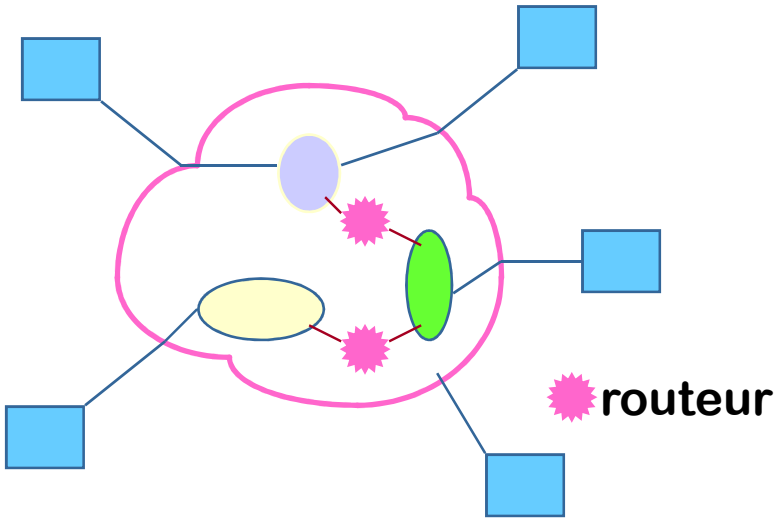
1. Intranet : un réseau d'entreprise dans lequel les mêmes technologies et protocoles que l'Internet sont mis en œuvres
   - Routeurs, protocoles TCP/IP, protocoles applicatifs : émail, web, …

2. Extranet : un Intranet qui offre des accès distants aux usagers/employés/partenaires de l'entreprise
   - Problème de sécurité

Structure Physique de l'INTERNET



Vue utilisateur



Vue réelle du réseau

Qui normalise l'Internet ?

- Technologie INTERNET développée par un organisme bénévole : l'IETF (Internet Engineering Task Force) organisé en 8 secteurs de recherche,

- Les normes sont appelées RFC (Request For Comment),
  - Exemple : RFC 791 (décrit IP) – RFC 793 (décrit TCP)
  - Documents gratuits accessibles à « www.ietf.org »

- Tout le monde peut proposer un RFC
  - L'IAB (Internet Activities Board) gère le processus d'acceptation des RFC

- les standards sont publiés par une association sans but lucratif l'internet society (1992)

Qui gère Internet

1. Normes techniques : IETF (internet Engineering Task Force)
   Les normes sont appelées RFC (Request For Comment),
   - Exemple : RFC 791 (décrit IP) – RFC 793 (décrit TCP)
   - Documents gratuits accessibles à « www.ietf.org »
2. Noms de domaines: ICANN (USA), RIPE (France)
   ICANN : Internet corporation for Assigned Names and Numbers;
3. Adresses IP, N°port, N°AS : ICANN depuis décembre 1998;
4. Réseaux : ISP (Internet Service Provider), NSP (Network Service Provider)
5. Fibres : Opérateurs télécoms
6. Serveurs, contenus : tout le monde (particuliers, entreprises, université, …)

Allocation des Adresses/Noms

Internet Corporation For Assigned Names and Numbers

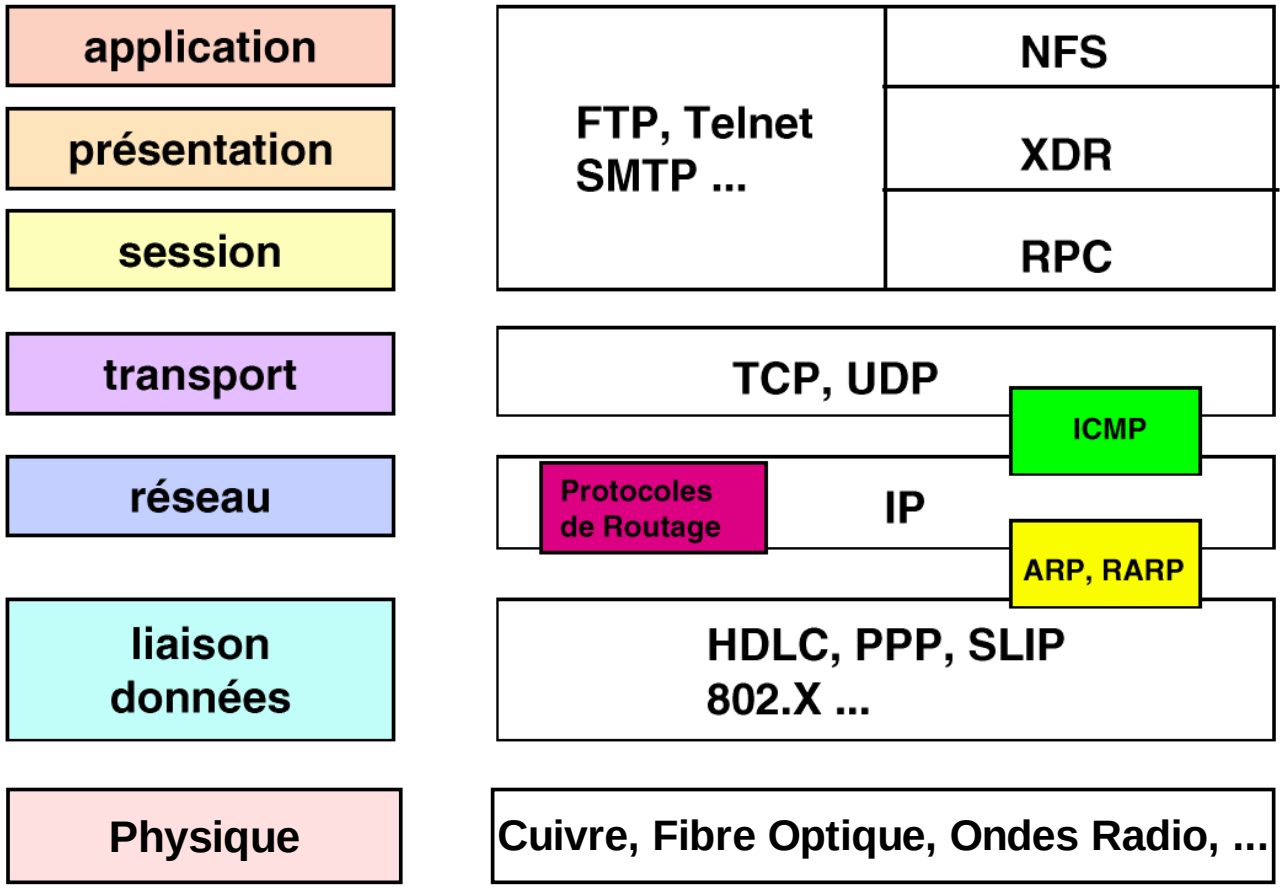
RIR
Regional Internet Registries

NIR
National Internet Registries

LIR
Local Internet Registries

End Users

Architecture TCP/IP



Normes et RFC

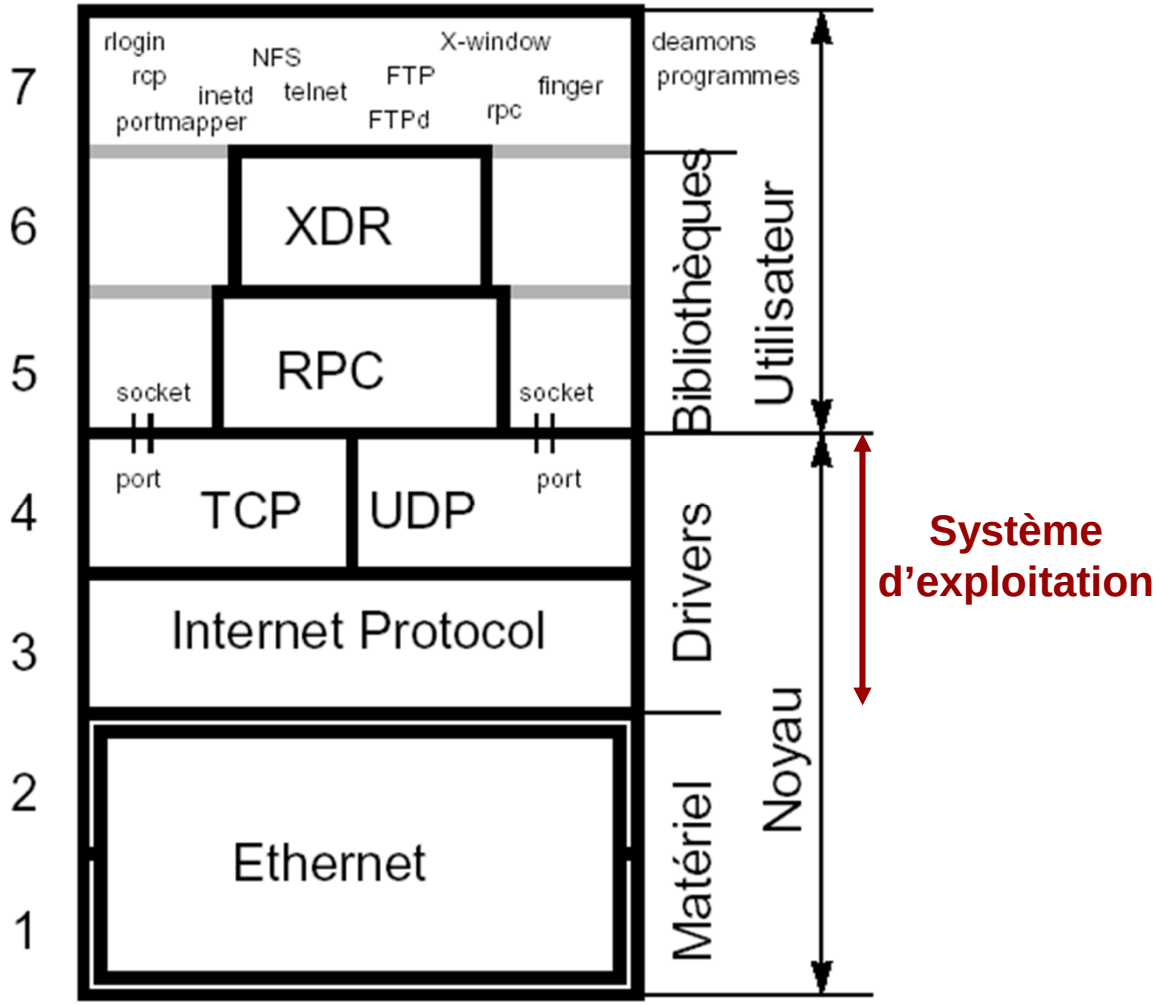
- Couche Liaison :
  - **SLIP : Serial Line IP** — **RFC 1055**
  - **PPP : Point to Point Protocol** — **RFC 1661**
- Couche Réseaux :
  - **IP : Internetworking Protocol** — **RFC 791 (v4) et RFC 2460 (v6)**
  - **ICMP : Internet Control Message Protocol** — **RFC 792**
  - **ARP : Adress Resolution Protocol** — **RFC 826**
  - **RARP : Reverse ARP** — **RFC 903**
  - **IGMP : Internet Group Management Protocol** — **RFC 1112**
- Protocoles Transport
  - **UDP : User Datagram Protocol** — **RFC 768**
  - **TCP : Transport Control Protocol** — **RFC 793**

Normes et RFC (suite)

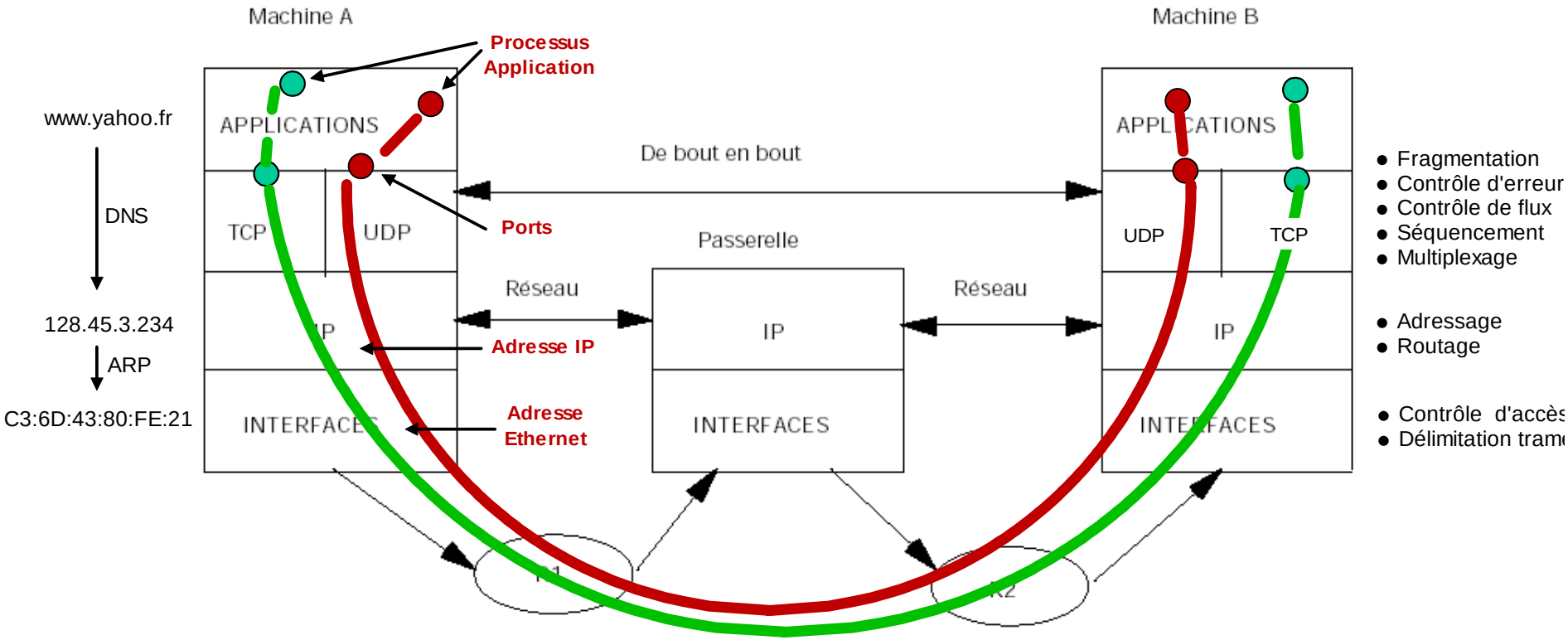
- Couche Application :

– **DNS : Domain Name Server**	**RFC 1034**	**UDP (53)**
– **HTTP : Hyper Text Transfer Protocol**	**RFC 2616**	**TCP (80)**
– **SMTP : Simple Mail Transfer Protocol**	**RFC 821**	**TCP (25)**
– **POP 3 : Post Office Protocol**	**RFC 1939**	**TCP (110)**
– **MIME : Multipurpose Internet Mail Extensions**	**RFC 2045**	**-**
– **FTP : File Transfer Protocol**	**RFC 959**	**TCP (20-21)**
– **TELNET**	**RFC 854**	**TCP (23)**
– **BOOTP : Bootstrap Protocol**	**RFC 951**	**UDP (67-68)**
– **DHCP : Dynamic Host Configuration Protocol**	**RFC 2131**	**TCP (546-547)**
– **SNMP : Simple Network Management Protocol**	**RFC 1157**	**UDP (161-162)**
– **RIP 2 : Routing Internet Protocol**	**RFC 2453**	**UDP (520)**
– **OSPF 2 : Open Shortest Path First**	**RFC 2328**	**-**
– **BGP : Border Gateway Protocol**	**RFC 1771**	**TCP (179)**
– **IMAP : Internet Message Access Protocol**	**RFC 2060**	**TCP (143)**
– **RTSP : Real Time Streaming Protocol**	**RFC 2326**	**TCP (554)**
– **NFS : Network File system**	**RFC 1094**	**UDP (2049)**

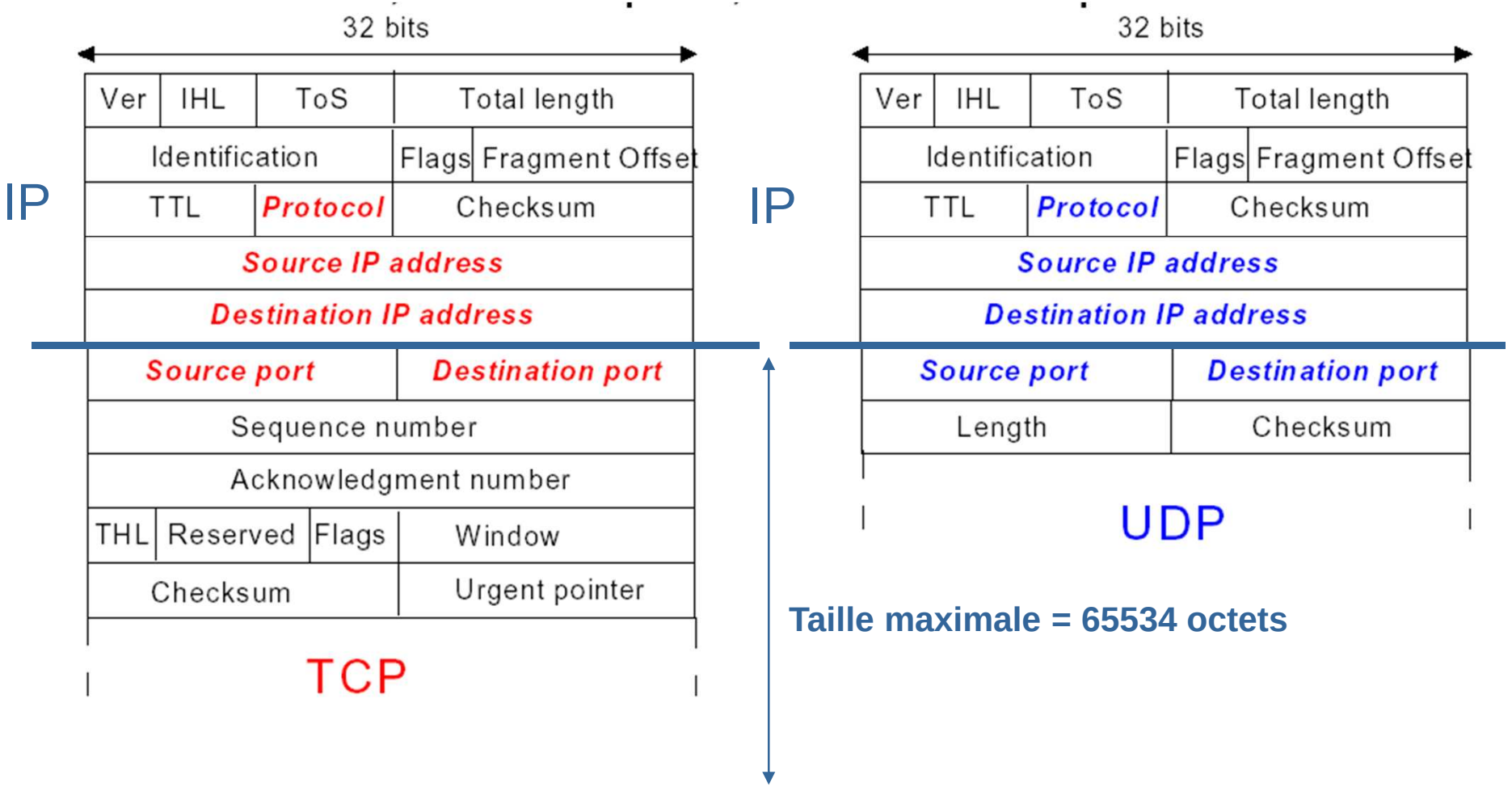
Architecture d'un terminal IP



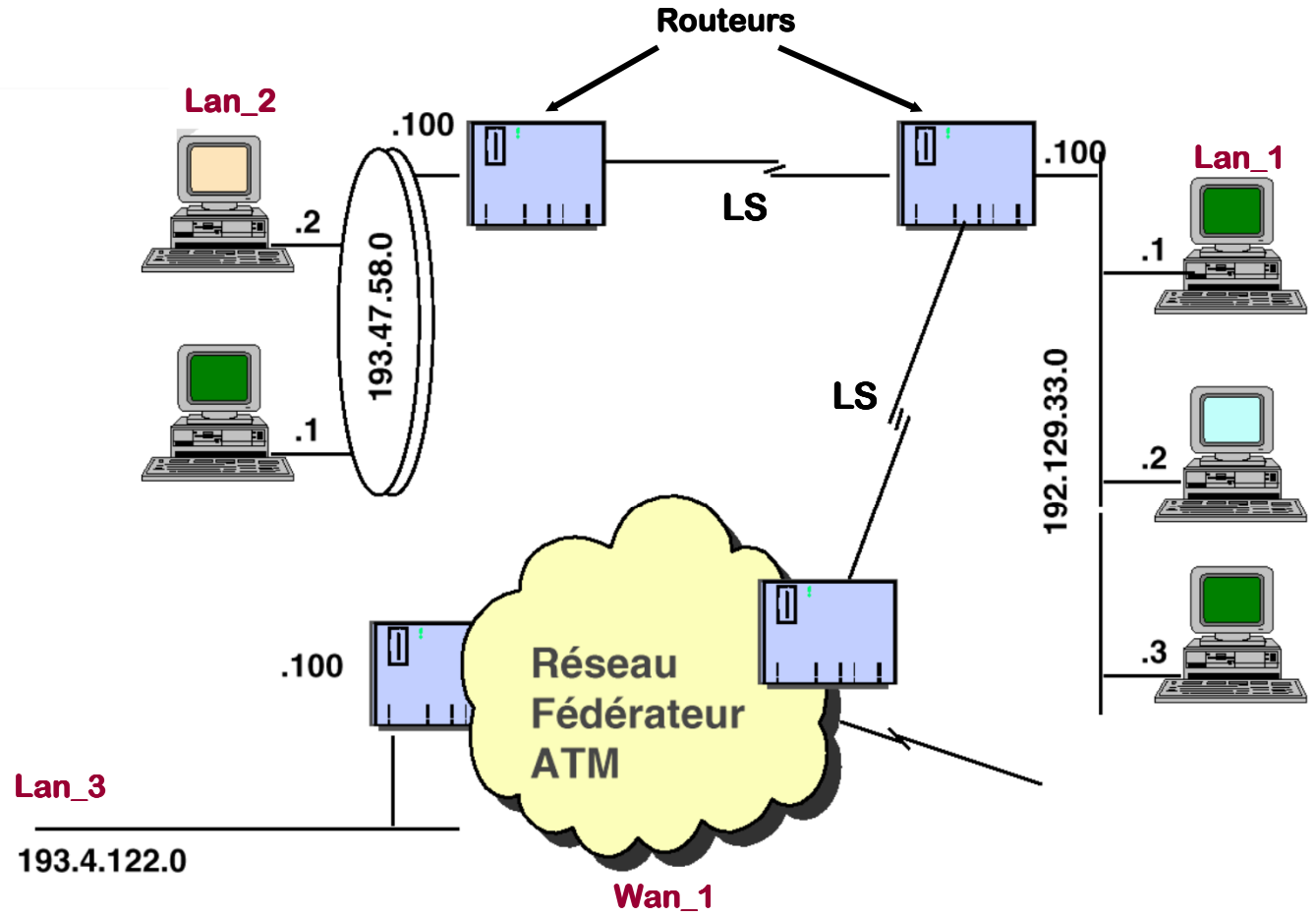
Communication client/serveur



Structure des Paquets IP

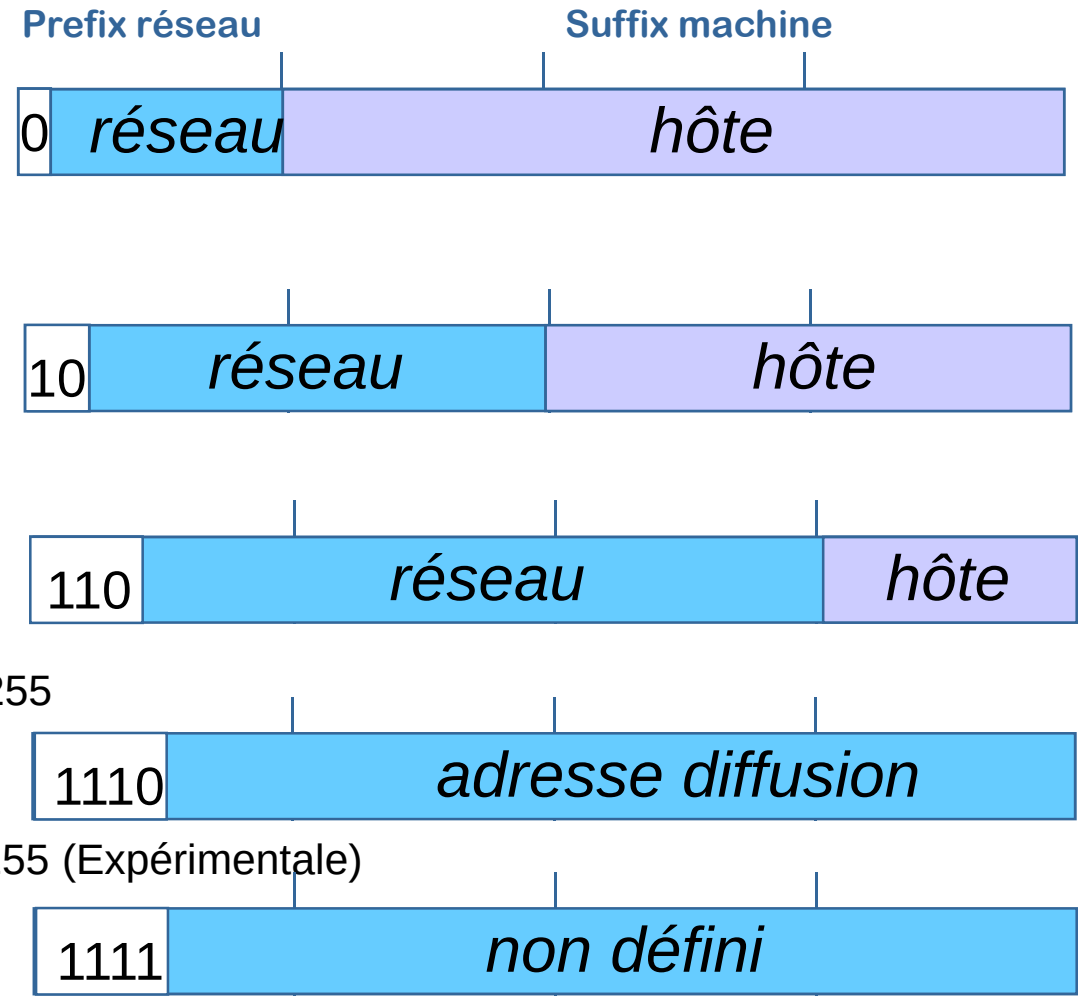


Adresse réseau



Classes d'adresses IP

- Classe A de 1.x.x.x à 127.x.x.x
  - 127 réseaux –
  - 16777214 machines
- Classe B de 128.0.x.x à 191.255.x.x
  - 16384 réseaux –
  - 65534 machines
- Classe C de 192.0.0x à 223.255.255.x
  - 2097152 réseaux –
  - 254 machines
- Classe D de 224.0.0.0 à 239.255.255.255 (multicast)
- Classe E de 240.0.0.0 à 255.255.255.255 (Expérimentale)



Adresses IP particulières

- **Adresse de diffusion** : **tous les champs sont à « 1 »**
  - **Exemple : 255.255.255.255**
  - **Diffusion sur tout le réseau (tous les sous-réseaux sont concernés)**

- **Adresse de diffusion dirigée** : **le champ «hostid» est tout à « 1 » et le champ « netid » est une adresse réseau spécifique** :
  - **Exemple : 192.20.0.255**
  - ⇒ **la diffusion concerne toutes les machines situées sur le réseau spécifié : 192.20.0.255**
  - ⇒ **désigne toutes les machines du réseau de classe C 192.20.0**

- **Adresse de boucle locale** :
  - **l'adresse réseau 127.0.0.1 est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Une adresse réseau 127 ne doit, en conséquence, jamais être véhiculée sur un réseau et un routeur ne doit jamais router un datagramme pour le réseau 127.**

- **Adresse de BOOTP (« hostid » et « netid » tout à zéro), l'adresse est utilisée au démarrage du système afin de connaître l'adresse IP (Cf RARP).**
  - **Exemple : 0.0.0.0**

Masque de réseau ou Netmask

- Masque du réseau : adresse IP particulière servant à identifier l'adresse du réseau à partir d'une adresse IP de machine.
  - Le masque d'un réseau de classe A = 255.0.0.0
  - Le masque d'un réseau de classe B = 255.255.0.0
  - Le masque d'un réseau de classe C = 255.255.255.0
  - Dans le cas d'un réseau découpé en sous-réseau : le masque est calculé en mettant tous les bits du préfix réseaux à la valeur binaire « 1 », et tous les bits associés au suffix à « 0 ».

- Adresses réseau : adresse IP dont la partie « hostid » ne comprend que des zéros;
  - => la valeur zéro ne peut être attribuée à une machine réelle : 192.20.0.0 désigne le réseau de classe C 192.20.0

- Adresse machine locale : adresse IP dont le champ réseau (netid) ne contient que des zéros;
  - Exemple 0.0.25.1

Netmask

- Permet à une station de savoir si la station destination est dans le même réseau qu'elle ou s'il lui faut envoyer son paquet au routeur qui l'acheminera,
- Exemple station A veut envoyer un paquet à une station B :
  - **@ IP A = 172.16.2.4**
  - **@ IP B = 172.16.3.5**
  - **@ netmask A : 255.255.0.0**
- La station A doit réaliser 3 opérations :
  1. **@ A AND @ netmask A = Res 1**
  2. **@ B AND @ netmask A = Res 2**
  3. **comparer Res 1 et Re 2**
     - **Si Res 1 = Res2 alors station sur le même réseau**
     - **Sinon station sur des réseaux distants**

Netmask (2)

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

172 . 16 . 2 . 4 (@ IP A)

10101100 . 00010000 . 00000010 . 00000100

11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0)

10101100 . 00010000 . 00000000 . 00000000 (@ du réseau classe B 172.16.0.0)

172 . 16 . 3 . 5 (@ IP B)

10101100 . 00010000 . 00000011 . 00000101

11111111 . 11111111 . 00000000 . 00000000 (mask A = 255.255.0.0)

10101100 . 00010000 . 00000000 . 00000000 (@ du réseau B 172.16.0.0)

Netmask (3)

Autre exemple @ IP C = 125.128.96.12

172 . 16 . 2 . 4	(@ IP A)
10101100 . 00010000 . 00000010 . 00000100	
11111111 . 11111111 . 00000000 . 00000000	(mask A = 255.255.0.0 - classe B)
10101100 . 00010000 . 00000000 . 00000000	(@ du réseau classe B 172.16.0.0)

125 . 128 . 96 . 12	(@ IP C)
01111111 . 10000000 . 01100000 . 00001100	
11111111 . 11111111 . 00000000 . 00000000	(mask A = 255.255.0.0)
01111111 . 10000000 . 00000000 . 00000000	(@ du réseau classe A 125.128.0.0)

Adresses IP Privées

- Classe A : 10.0.0.0 - 10.255.255.255
- Classe B : 172.16.0.0 - 172.31.255.255
- Classe C : 192.168.0.0 - 192.168.255.255

Problème des adresses IPv4

- L'assignation d'une classe par bit, signifie : la classe A prend 1/2 des adresses, la classe B 1/4, la classe C 1/8 etc.
- Problèmes avec une telle assignation :
  1. Gaspillage
  2. Saturation dans les routeurs
  3. Pénurie des adresses encore libres

- Solutions ?

1. Utiliser les adresses IP privées avec un protocole de translation d'adresse (NAT: Network Address Translation)
2. Fractionner les blocs d'adresses plus finement : « Subnetting » ou « sous-adressage »
   - **conserver la taille à 32 bits mais …**
3. Augmenter la taille du champ adresse :
   - **Exemple : IP version 6 (décembre 1998) : champ adresse de 128 bits**
   - **conséquence : incompatibilité entre les machines**

« NAT »

- **Network Address Translation :**

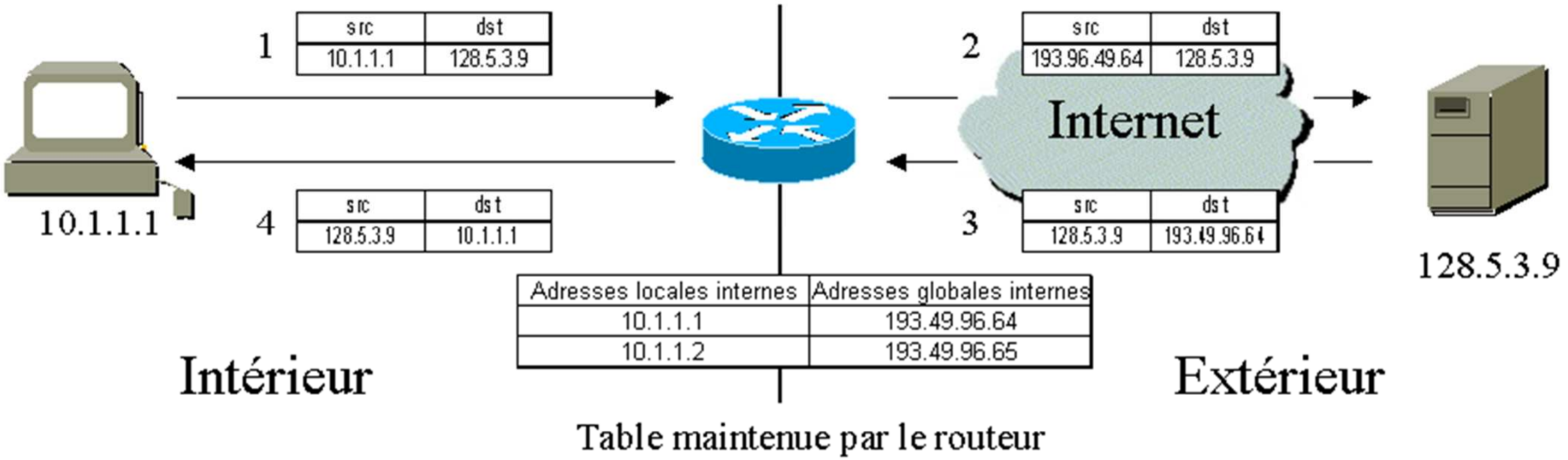


Table maintenue par le routeur

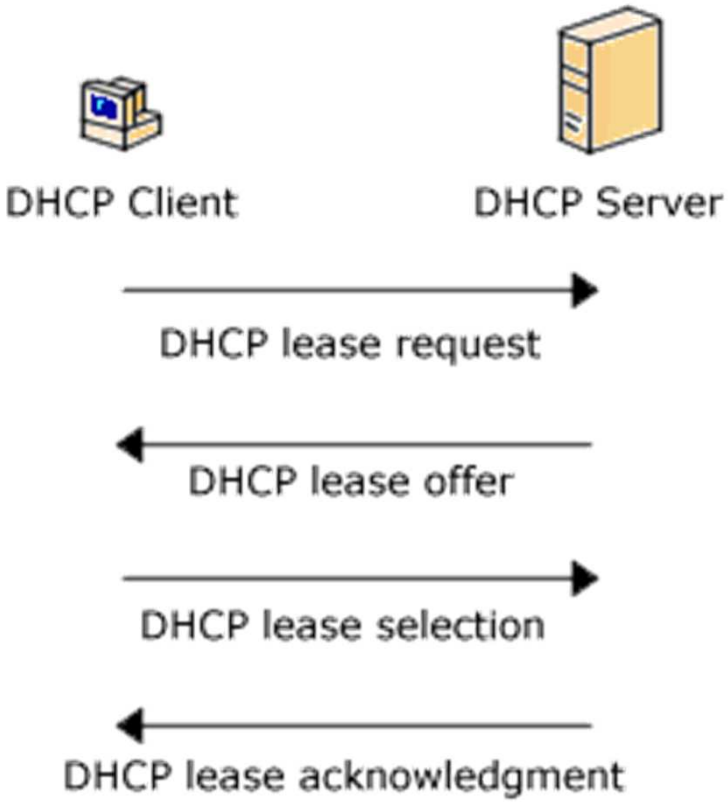
Attributions des adresses IP

- **Pour communiquer dans un réseau IP, les hosts doivent connaître :**
  - L'adresse IP du host
  - Le masque de leur réseau
  - L'adresse IP de la passerelle (Gateway) (optionnel)
  - L'adresse IP du serveur de noms (DNS) (optionnel)

- **Configuration statique :**
  - Configuration manuelle et permanente.
  - requise pour les serveurs et routeurs
  - Commandes systèmes **ifconfig** (unix) - **netsh** (windows)

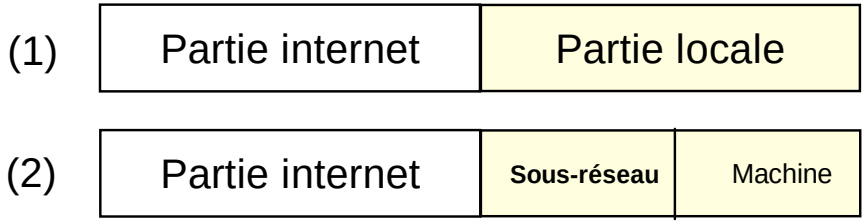
- **Configuration dynamique** :
  - Simplicité et optimisation des adresses IP
  - Adaptée pour les terminaux nomades
  - Utilisation d'un serveur de configuration interrogé par les terminaux au démarrage
  - Les clients et le serveur communique au moyen d'un protocole (règles d'échange et format de messages valides) **DHCP** (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP)



Subnetting

- Constat : Un site ne contient pas un réseau mais un ensemble de réseaux (exemple : UVSQ)
- Solution : scinder une classe en sous-réseaux (ou segment):
  - La partie numéro de machine devient le numéro de sous-réseau et le numéro de la machine dans ce sous-réseau,
  - Combien de bits (n) utiliser pour représenter les sous-réseaux ?
    - Si (p) sous-réseaux à représenter alors $p \geq (2^n)$
  - Nombre de bits alloués au numéro de sous-réseau est configurable : c'est le « sub-netmask » ou simplement le « netmask » du sous-réseau



Subnetting
Exemple

- Soit un réseau d'entreprise de classe B = 130.96.0.0 constitué de 10 sous-réseaux locaux.

- Pour identifier 10 sous-réseaux, combien de bits faut il prendre de la partie Host-id ?
  - 3 bits ? => 2^3 = 8 (insuffisant !!!)
  - 4 bits ? => 2^4 = 16 (Oui !!!)

  - Soit : 2^n (2 puissance n)

- Masque de sous-réseau = 255.255.240.0
- Exemple d'adresse de diffusion restreinte = 130.96.175.255 pour le sous-réseaux de net-id = 130.96.160.0

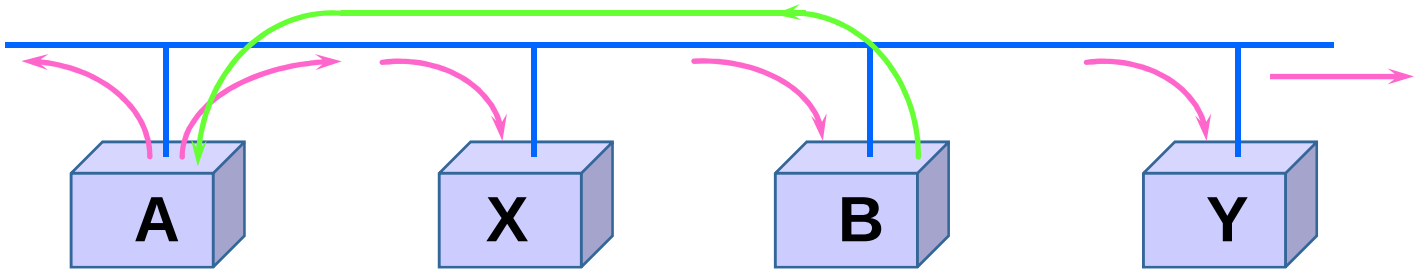
Résolution des adresses

- Pourquoi ?
  - Dans un Intranet ou Internet, les **communications** entre applications se font au moyen des adresses IP des hosts (et des n°de ports).
  - Dans un réseau local, **l'acheminement** des données se fait au moyen des adresses physiques des émetteurs et des récepteurs.
  - L'unité de transfert est la Trame Ethernet (et non le paquet IP)

  - Les adresses IP sont obtenues par l'interrogation d'un serveur : le **DNS**
  - Comment obtenir l'adresse physique d'une machine distante en connaissant son adresse IP ?
- La Solution :
  - ARP : Address Resolution Protocol
  - utiliser un protocole de type requête/réponse
  - utilise le principe de la diffusion sur le réseau local (broadcast)
  - l'association adresse physique - adresse IP de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache,

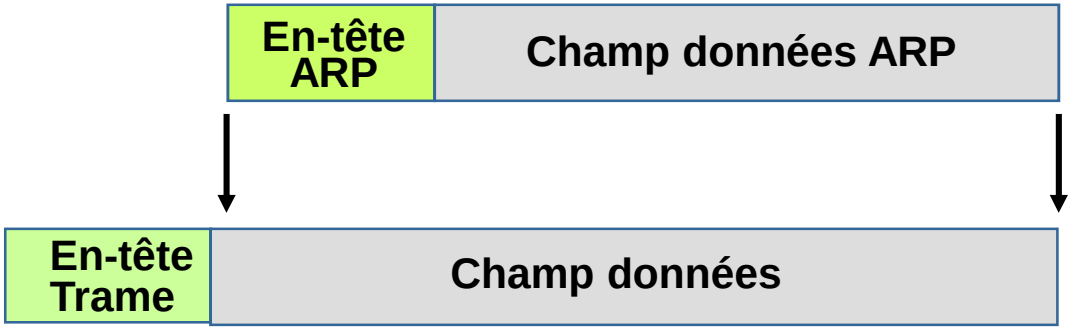
ARP

- L'association adresse physique - adresse IP de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache,

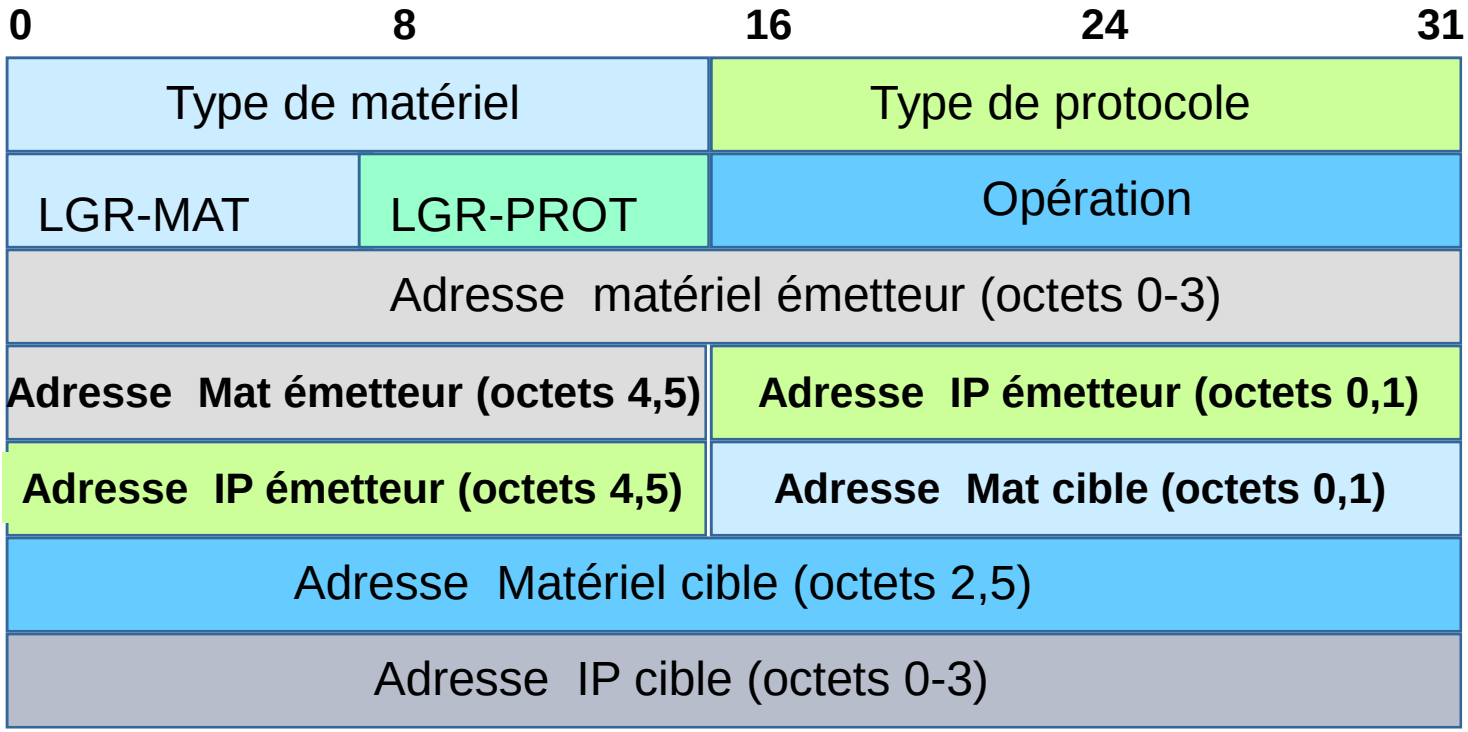


- Pour connaître l'adresse physique de B (PB) à partir de son adresse IP (IB), la machine A diffuse une requête ARP qui contient l'adresse IP de B (IB) vers toutes les machines;
- la machine B répond avec un message ARP qui contient la paire (IB, PB).
- Rem : champ type de la trame Ethernet: 0806 pour ARP

ARP : encapsulation



Format du message ARP

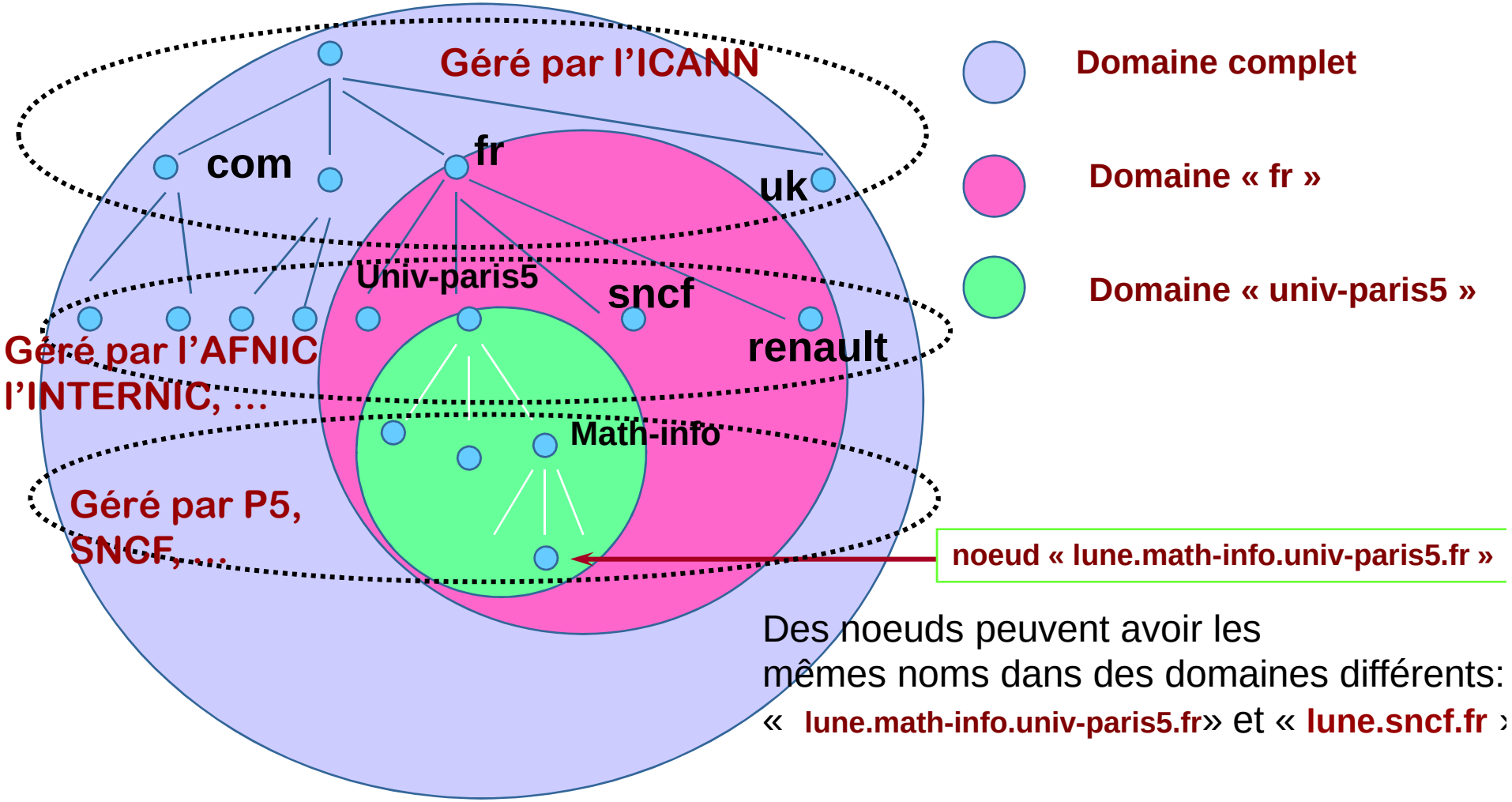


Nommage des ressources

- Nommage des ressources du réseau : utiliser un NOM SYMBOLIQUE plutôt qu'une adresse décimale :
  - brune.prism.uvsq.fr 193.51.25.130
  - www.yahoo.fr 10.25.123.68
  - Unicité des adresses => unicité des noms
  - Il existe un « plan de nommage » hiérarchique mondiale et un « service de noms » mondial : le DNS (Domain Name System)

Le domaine

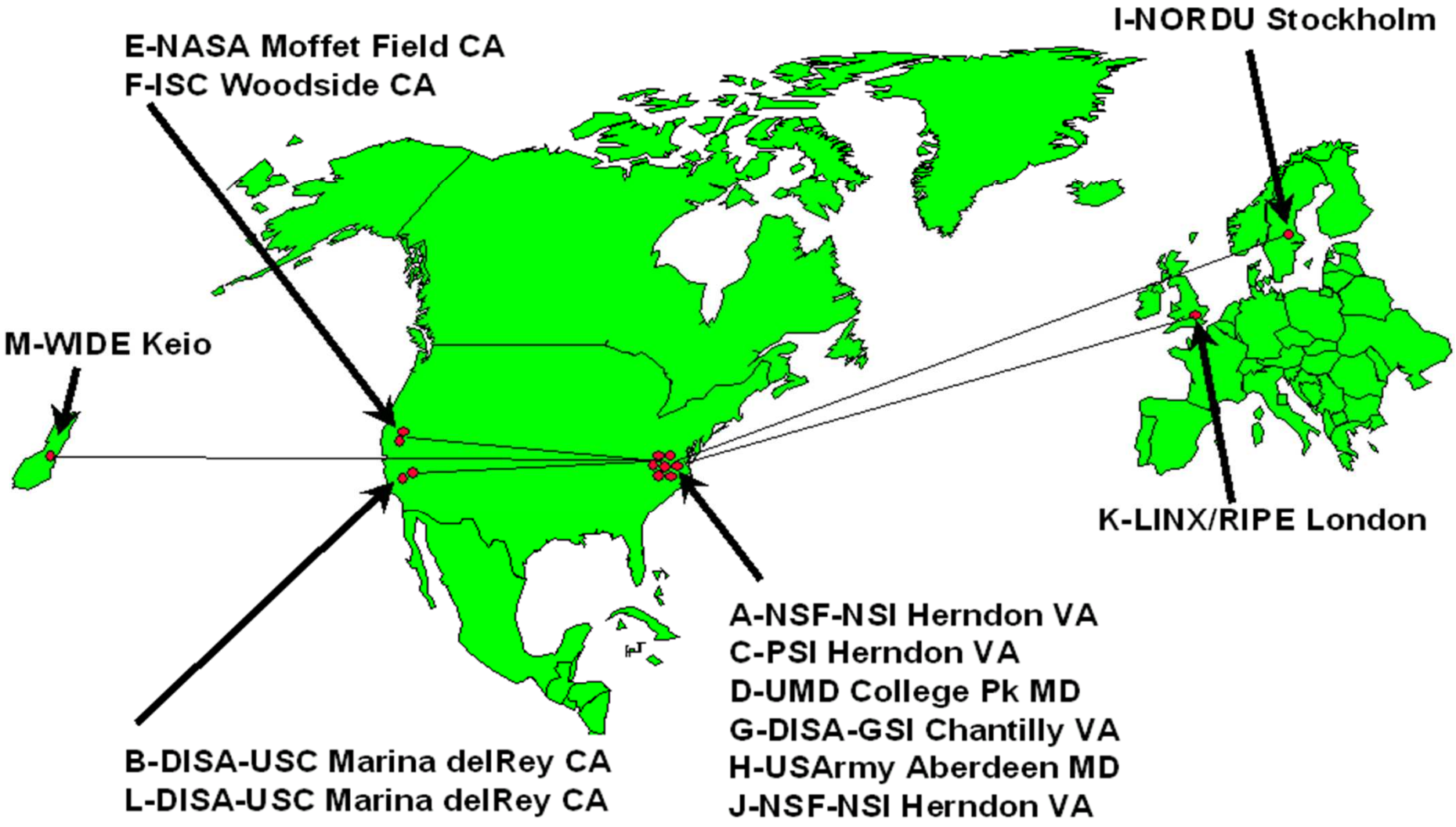
Un domaine est un sous-arbre de l'espace nom de domaine



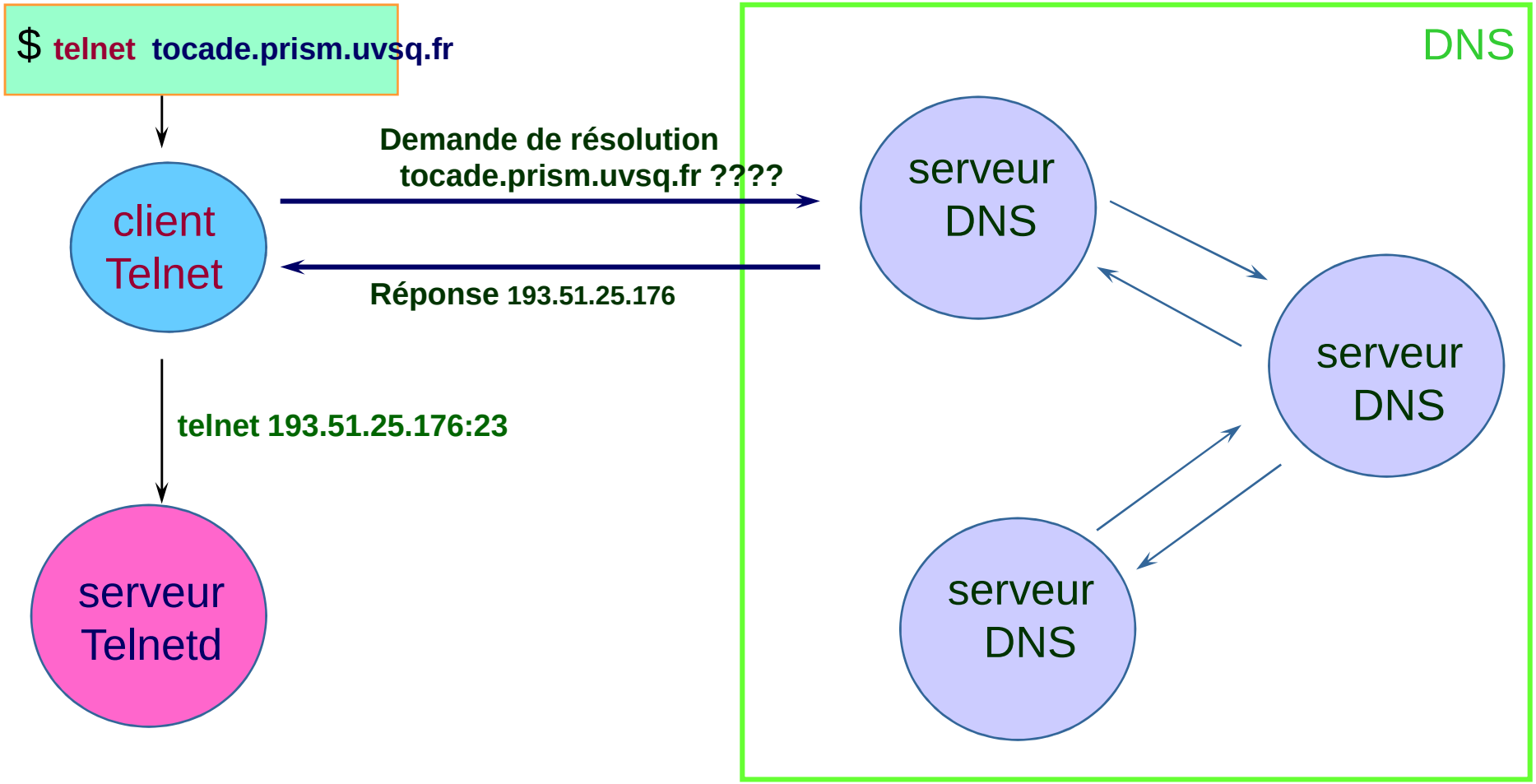
Des noeuds peuvent avoir les mêmes noms dans des domaines différents: « **lune.math-info.univ-paris5.fr**» et « **lune.sncf.fr** »

DNS Root Servers

Designation, Responsibility, and Locations



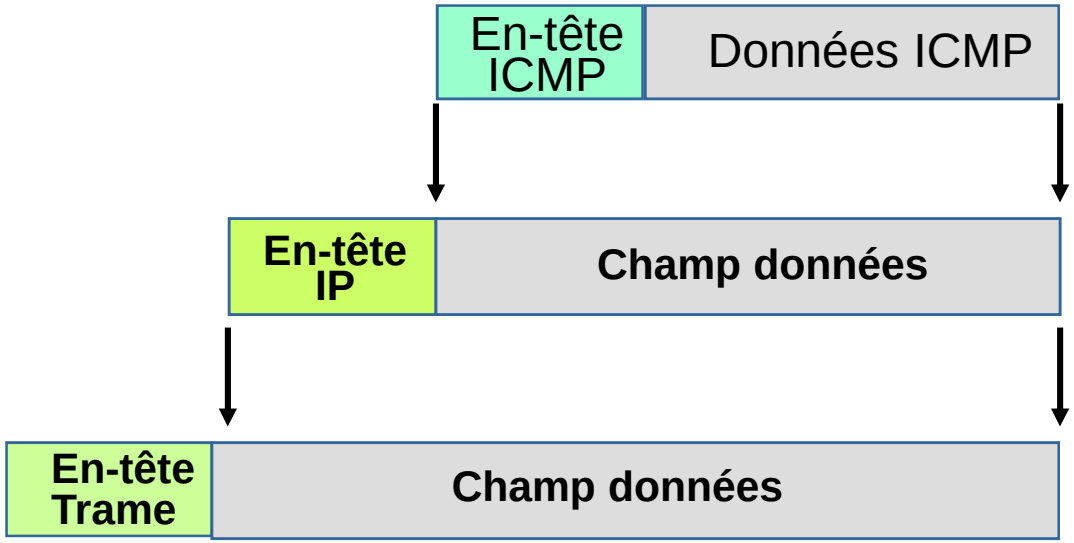
Principe (illustration)



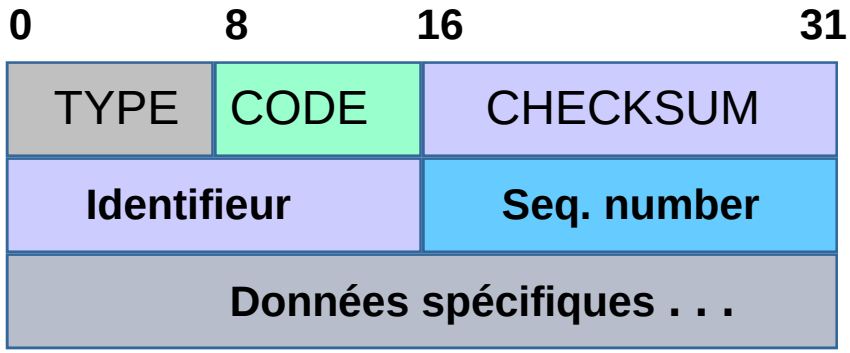
Protocole ICMP

- Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de commande ou des messages d'erreurs vers d'autres machines ou routeurs.
- ICMP rapporte les messages d'erreur à l'émetteur initial.
- Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dûes à des problèmes d'interconnexions rencontrées sur l'Internet :
  - **machine destination déconnectée,**
  - **durée de vie du datagramme expirée,**
  - **congestion de routeurs intermédiaires.**
- Si un routeur détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.
- Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'internet.
- Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP (évite l'effet cummulatif).

ICMP : encapsulation



ICMP : format des messages



En-tête ICMP

TYPE 8 bits; type de message

CODE 8 bits; informations complémentaires

CHECKSUM 16 bits; champ de contrôle

IDENTIFIER (16 bits) et SEQUENCE NUMBER (16 bits) sont utilisés par l'émetteur pour contrôler les réponses aux requêtes, (CODE = 0).

ICMP : type de messages

TYPE	Message ICMP
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
11	Time Exceeded (TTL)
12	Parameter Problem with a Datagram

TYPE	Message ICMP
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Reply (obsolète)
17	Address Mask Reques
18	Address Mask Reply

ICMP : les messages d'erreur

- Lorsqu'une passerelle émet un message ICMP de type destination inaccessible, le champ CODE décrit la nature de l'erreur :
  - 0 Network Unreachable
  - 1 Host Unreachable
  - 2 Protocol Unreachable
  - 3 Port Unreachable
  - 4 Fragmentation Needed and DF set
  - 5 Source Route Failed
  - 6 Destination Network Unknown
  - 7 Destination Host Unknown
  - 8 Source Host Isolated
  - 9 Communication with desination network administratively prohibited
  - 10 Communication with desination host administratively prohibited
  - 11 Network Unreachable for type of Service
  - 12 Host Unreachable for type of Service