RESEAU II

Protocoles

OUTILS RÉSEAU

Ping, traceroute, nslookup…

Ping

- Ping : *Packet INternet Groper*
- But : vérifier si une machine est accessible via le réseau
  - Tester le routage
  - Test la source et destination
- Protocole : ICMP encapsulé dans un datagramme IP
  - RFC 792, 1981
- Fonctionnement
  - 1- A intervalles réguliers (chaque sec.), la source envoie un "echo request" à la destination.
    - ICMP type 8
  - 2- La destination répond par un "echo reply".
    - ICMP type 0

ICMP

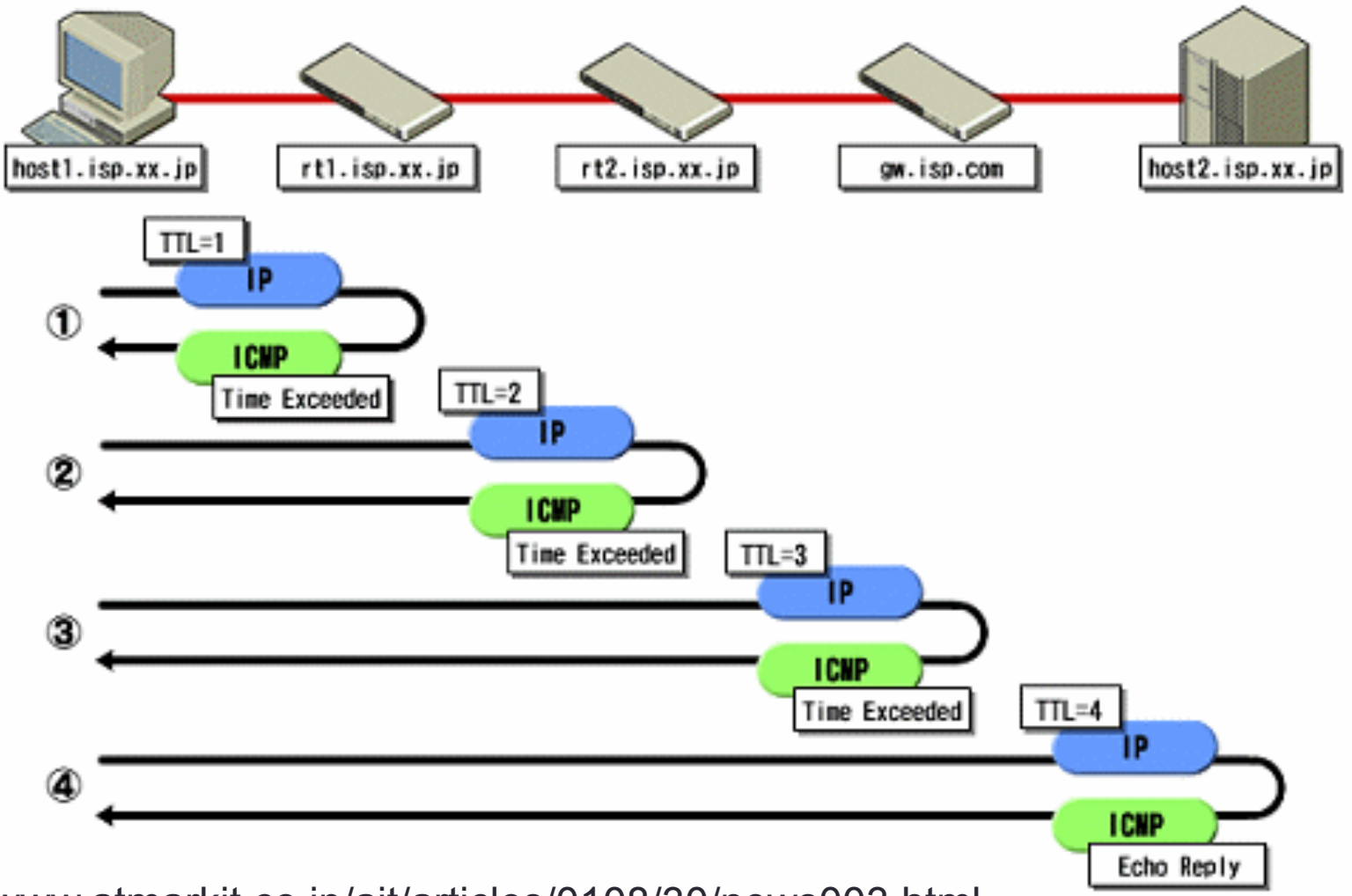
	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

https://en.wikipedia.org/wiki/Ping_(networking_utility)

Traceroute

- But : permettre de suivre les chemins qu'un datagramme IP de la source à la cible
- Protocole : ICMP (ou paquet UDP ou TCP)
- Fonctionnement :
  - Envoyer un echo-request avec de plus en plus grand en commençent à 1
  - Chaque passage de routeur décrémente le TTL avent le le transmettre au routeur suivant
  - Lorsque le TTL est à 0, le routeur envoie un paquet ICMP "time to live exceeded" à la source
  - Découvert des routes de proche en proche

Exemple



http://www.atmarkit.co.jp/ait/articles/0108/30/news003.html

Netstat

- pour « **net**work **stat**istics »
- But : afficher des informations sur les connexions réseau, les tables de routage, des statistiques sur les interfaces

Exemple 1

```
netstat -i
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0 1201958408      0      0    144 1233359697      0      0      0 BMRU
eth1       1500   0 41647044       0      0      0 32555621       0      0      0 BMRU
lo        16436   0 16333175       0      0      0 16333175       0      0      0 LRU
```

Exemple 2

```
$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     *               255.255.255.0   U         0 0          0 eth0
193.52.29.0     *               255.255.255.0   U         0 0          0 eth1
default         routuni121-2.un 0.0.0.0         UG        0 0          0 eth1
```

Exemple 3

```
$ netstat -s
Ip:
    300150605 total packets received
    2 with invalid headers
    2270 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    300146167 incoming packets delivered
    392882210 requests sent out
    32 dropped because of missing route
    11 fragments dropped after timeout
    2534 reassemblies required
    636 packets reassembled ok
    11 packet reassembles failed
Icmp:
    7655 ICMP messages received
    1473 input ICMP message failed.
```

Dig

- But : Permettre d'interroger les serveurs DNS pour obtenir les informations définies pour un domaine déterminé
- Remplacant d'NSLookup qui n'est plus maintenu
- Protocole : DNS
  - RFC 883, 1983 → RFC 1035, 1987
- Fonctionnement
  - Interroge le DNS enregistrer sur la machine ou un DNS spécifié en ligne de commande

Exemple 1

```
dig www.univ-lemans.fr

; <<>> DiG 9.8.3-P1 <<>> www.univ-lemans.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28425
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.univ-lemans.fr.                IN      A

;; ANSWER SECTION:
www.univ-lemans.fr.        17754    IN      CNAME    cms-fo3.univ-lemans.fr.
cms-fo3.univ-lemans.fr.    17754    IN      A        195.221.244.60

;; Query time: 48 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Oct 15 21:32:44 2015
;; MSG SIZE  rcvd: 74
```

Exemple 2

```
dig MX www.univ-lemans.fr

; <<>> DiG 9.8.3-P1 <<>> MX www.univ-lemans.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52998
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.univ-lemans.fr.            IN        MX

;; ANSWER SECTION:
www.univ-lemans.fr. 12182      IN        CNAME     cms-fo3.univ-lemans.fr.

;; AUTHORITY SECTION:
univ-lemans.fr.                3600      IN        SOA       ns1.univ-lemans.fr.
sbourdai.ns1.univ-lemans.fr. 2015101506 14400 3600 2419200 28800

;; Query time: 66 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Oct 15 21:33:12 2015
;; MSG SIZE  rcvd: 107
```

Exemple 3

```
dig MX univ-lemans.fr

; <<>> DiG 9.8.3-P1 <<>> MX univ-lemans.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27624
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;univ-lemans.fr.                    IN      MX

;; ANSWER SECTION:
univ-lemans.fr.             2365    IN      MX      10 mxa.relay.renater.fr.
univ-lemans.fr.             2365    IN      MX      10 mxc.relay.renater.fr.
univ-lemans.fr.             2365    IN      MX      10 mxd.relay.renater.fr.
univ-lemans.fr.             2365    IN      MX      10 mxb.relay.renater.fr.

;; Query time: 37 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Oct 15 21:33:31 2015
;; MSG SIZE  rcvd: 126
```

DNS

Introduction

- DNS (1984)
  - Système de nommage Internet
  - **Domain Name System**
- Notions de
  - **Nom de domaine**
  - **Domaine de zone**
  - **Arborescence**

Pourquoi ?

- Les ordinateurs connectés au réseau Internet communiquent en utilisant un protocole TCP/IP
- Chaque hôte du réseau est identifié par une adresse logique
  - Un nombre de 32 bits
  - IP : **192.168.1.36**
- Notation numérique n'est pas commode pour l'utilisateur
  - Difficile de retenir une longue suite de chiffres
- Plus aisé de leur attribuer des noms symboliques
  - www.univ-lemans.fr
- Nécessité de disposer d'un service de mise en correspondance nom symbolique ←→ adresse logique

Les premières années d'Internet

- La mise en correspondance était assuré en utilisant un fichier unique centralisé (/etc/hosts)
- Ce fichier donnait les noms de toutes les machines ainsi que leurs adresses IP
- Il fallait le télécharger et et le stocker sur chaque machine
- « Relativement » efficace dans les années 70
  - Quelques centaines d'ordinateurs connectés au réseau
- Atteint ses limites plusieurs millions de machines :
  - temps de diffusion des informations élevé
  - correspondance statique
  - forte probabilité de collisions de noms

DNS

- Modèle en arborescence
  - Similaire à celui des systèmes de fichiers et de répertoires
  - Avec une gestion décentralisée des données
  - Chaque site est responsable des données de sa zone
- Fournir d'autres informations
  - Temps de validité des informations,
  - Les relais de messagerie,
  - Les alias de machines, etc...,
- Le DNS = une base de données distribuée
  - Permet à certaines machines de contrôler certains segments de la base de données
  - Accessible avec un mécanisme client-serveur.
  - Système de réplication assure une fiabilité raisonnable
  - Système de caches permet d'augmenter la performance

Nom de domaine

- Le nom de domaine est une partie intégrante de l'adresse de toute ressource Interne identifier par son URL
- Chaque machine fait partie d’un domaine
- Nom de domaine = un identifiant unique lié à une entité dont les ordinateurs sont reliés au réseau Internet
- Constitué d'éléments séparés par un "."
  - analogie avec le "/" ou "\" dans un système de fichiers pour localiser un répertoire

Nom de domaine exemple

- Dans un réseau local, les machines peuvent être identifiées par leurs seuls noms
  - Commande "hostname"
- A l'échelle d'Internet, ces noms doivent être concaténés avec le nom du domaine dans lequel elles sont déclarées

- Nom du domaine : afnic.fr
  - Nom local de la machine : www
  - Nom de la machine dans le DNS : www.afnic.fr

  - Nom local de la machine : ftp
  - Nom de la machine dans le DNS : ftp.afnic.fr

Information

- L'information sur la correspondance nom et adresse IP est stockée dans la base de données du domaine
- la base de données du domaine afnic.fr va contenir des informations du type :

nom de machine :	**ftp.afnic.fr**	=>	adresse IP :	**192.134.4.13**
nom de machine :	**relay1.afnic.fr**	=>	adresse IP :	**192.134.4.17**
nom de machine :	**www.afnic.fr**	=>	adresse IP :	**192.134.4.11**
adresse IP :	**192.134.4.11**	=>	nom de machine :	**www.afnic.fr**

Domaine vs URL

- Important de faire la différence entre **nom de domaine** et **URL**
- Un nom de domaine peut être une partie d'une URL
- URL permet de localiser une ressource (une machine, un fichier, une boîte de messagerie électronique, etc...) sur internet
- Par exemple le nom de domaine abcd.fr :

  http://www.abcd.fr
  http://www.tot3.abcd.fr/doc
  http://abcd.fr/info/pub/prod.htm

  - sont des ressources web (pages web) localisées dans des machines du domaine abcd.fr et du sous-domaine tot3.abcd.fr

  root@abcd.fr
  info@www.abcd.fr

  - sont des boîtes de courrier électronique associées aux utilisateurs root et info

Organismes du nommage

Top-Level Domain

- Organisation hiérarchique
- TLD (Top-Level Domain) sont les domaines de premier niveau
  - Situés juste en dessous de la racine dans l'arbre de nommage
  - Leur structure et les modalités de leur gestion → RFC 1591
- Les TLD peuvent être subdivisés en deux catégories :
  - Domaines de 1er niveau nationaux ou ccTLD (country-code TLD)
  - Domaines de 1er niveau génériques gTLD (generic TLD)
- Jusqu'en 1998, la délégation de gestion d'un TLD → l'IANA (Internet Assigned Numbers Authority)
- Depuis lors → ICANN (Internet Corporation for Assigned Names and Numbers).

Country-code TLD

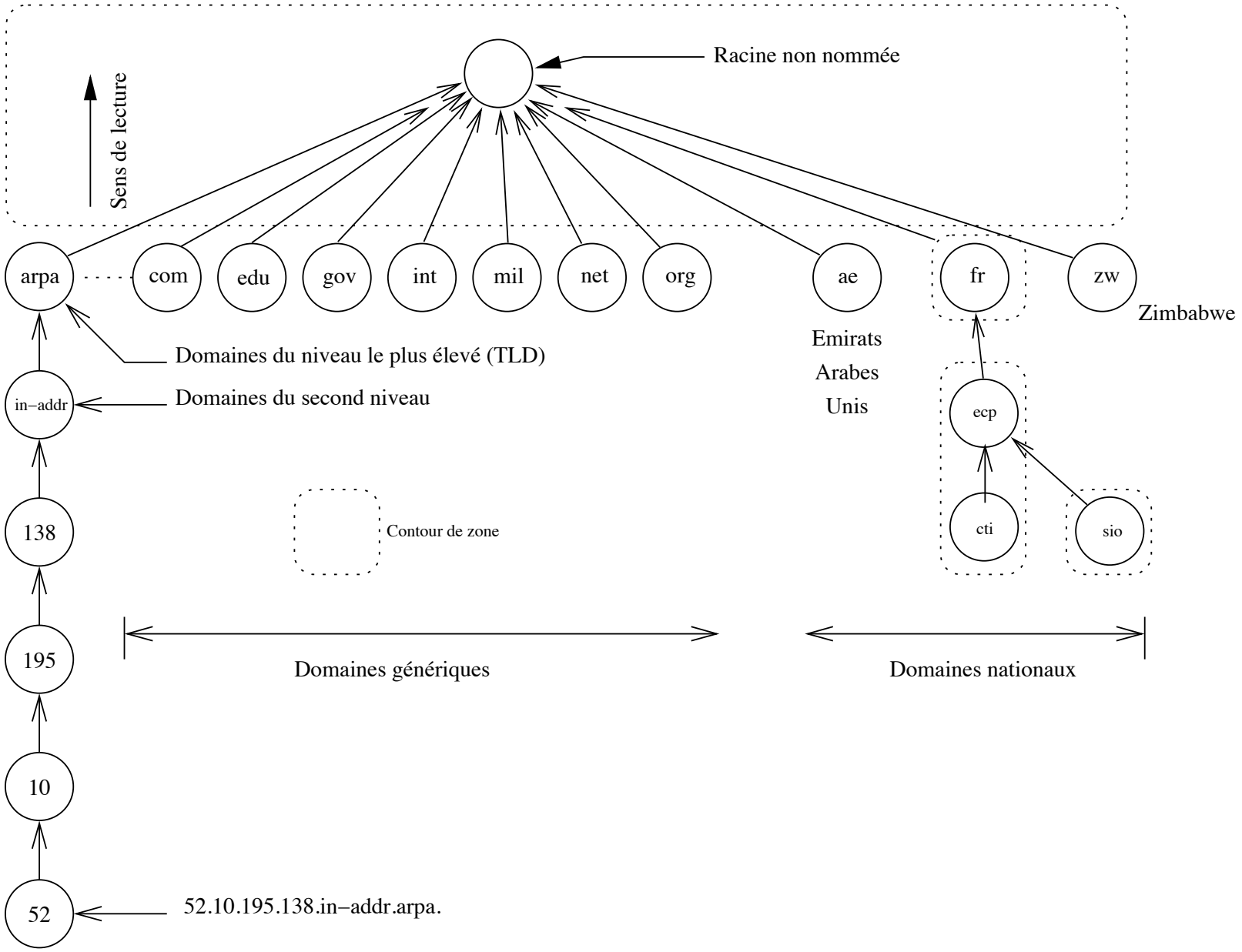
- Domaines nationaux
- Les ccTLD sont codés avec deux lettres suivant le code ISO 3166 de chaque pays
  - exemples :
    - fr pour la France,
    - it pour l'Italie,
    - sn pour le Sénégal…
- L'attribution d'un nom de domaine est du ressort de l'institution à qui cette mission a été confiée
- Les attributions sont effectuées en fonction de règles et conditions qui varient de pays à pays

Generic TLD

- Domaines génériques
- Permettent de regrouper des domaines de second niveau en fonction de
  - la nature ou
  - des secteurs d'activité
- Exemples:
  - com pour les entreprises,
  - edu pour les établissements du secteur de l'éducation U.S.,
  - org pour les organisations et en général pour ce qui n'est pas classable ailleurs, etc...)

Generic TLD

- Sept nouvelles extensions lancées en 2001/2002 :
  - aero pour les entreprises du secteur de l'aéronautique
  - biz pour les entreprises commerciales
  - coop pour les coopératives
  - info pour les entreprises spécialisées dans l'information
  - museum pour les musées
  - name pour les individus
  - pro pour les professions libérales


Racine non nommée
Sens de lecture
arpa
com
edu
gov
int
mil
net
org
ae
fr
zw
Zimbabwe
Emirats
Arabes
Unis
Domaines du niveau le plus élevé (TLD)
Domaines du second niveau
in−addr
ecp
cti
sio
138
Contour de zone
195
Domaines génériques
Domaines nationaux
10
52
52.10.195.138.in−addr.arpa.

Allocation des adresses Internet

Qui alloue les adresses IPv4 ?

- Adresses IP attribuées par des organismes agréés par l'ICANN
- **L'ICANN** délègue des pouvoirs d'attribution d'adresses IP à des registres régionaux (RIR : Regional Internet Registries)
- Les **RIR** attribuent des adresses IP aux registres locaux (LIR : Local IR)
- Les **LIR**
  - sont en général des fournisseurs de service Internet
  - se chargent de l'attribution d'adresses IP aux utilisateurs finaux
- Compte tenu de la pénurie actuellement d'adresses IP, les LIR s'efforcent d'attribuer aux utilisateurs finaux le nombre exact d'adresses dont ils ont besoin

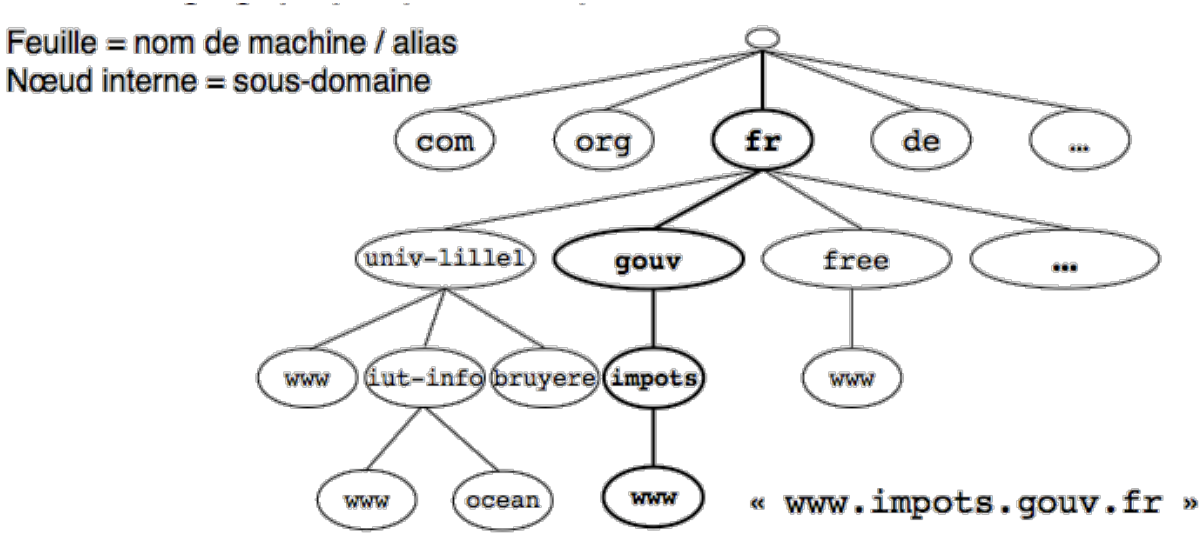
Regional Internet Registries (RIR)

- 3 RIR historiques :
  - APNIC (Asia Pacific Network Information Centre) chargé de l'attribution d'adresses IP dans la zone Asie - Pacifique;
  - ARIN (American Registry for Internet Numbers) qui a en charge les Amériques et une partie de l'Afrique subsaharienne;
  - RIPE NCC (Réseaux IP Européens - Network Coordination Centre) qui a en charge l'Europe, le Moyen-Orient, l'ex-URSS et la partie de l'Afrique non couverte par ARIN.
- 2 « nouveaux » Pour l'Afrique et l'Amérique Latine :
  - AfriNIC (African Regional Network Information Centre), 2005
  - LACNIC (Latin American and Caribbean IP address Regional Registry), 2001

Arborescence

Arbre de nommage

- Le DNS est organisé sous forme d'un arbre renversé avec comme éléments :
  - La racine (root) constitue le sommet de l'arbre
  - Des nœuds qui représentent des domaines
    - identifiés chacun par un label (exemple : fr, nl, sn, com, etc...) .

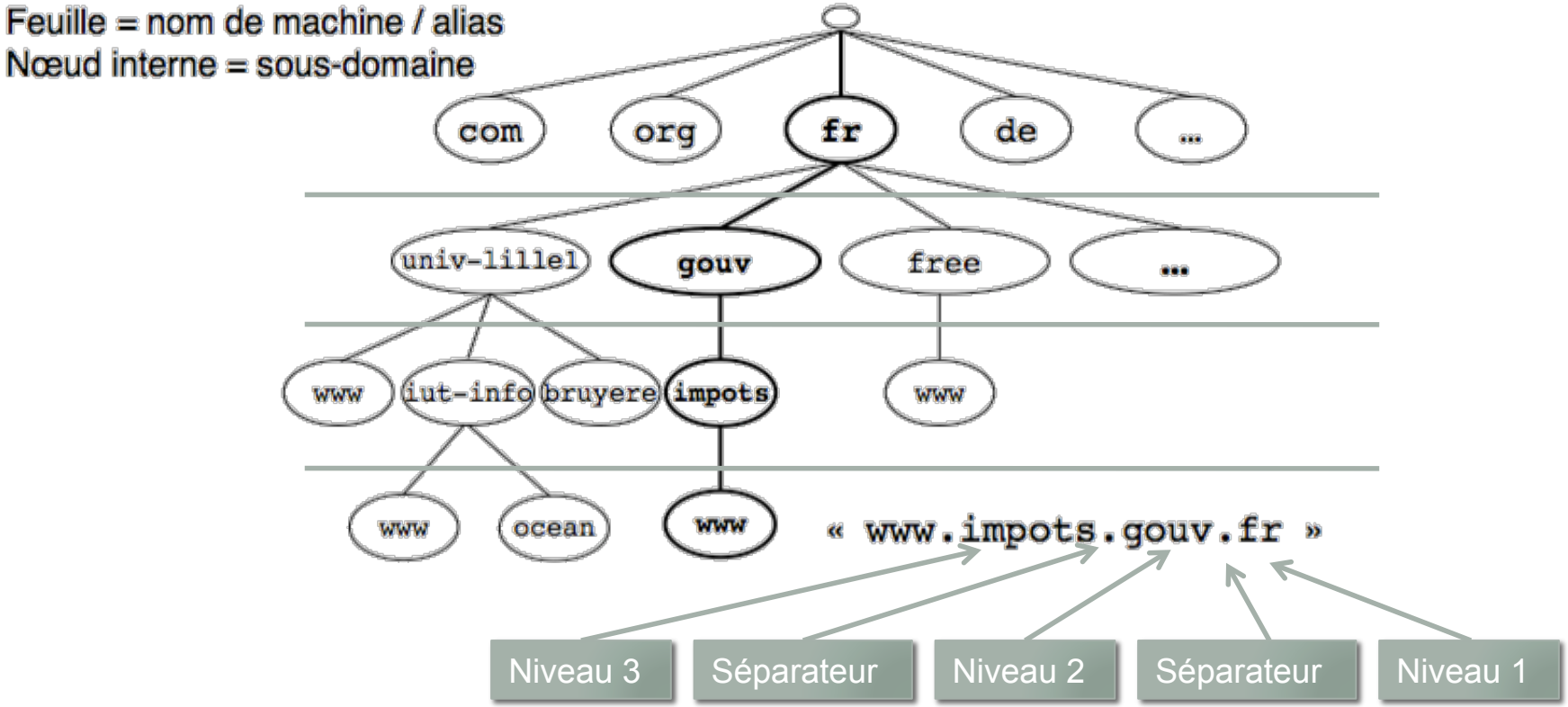


Arbre de nommage

- Informations des éléments de chaque nœud sont stockées dans une base de données
  - BD propre au nœud et gérée par celui-ci
- La base de données de la racine et les nœuds forment un système d'informations hiérarchique distribué
- Dans un système de fichiers, un répertoire peut contenir des sous-répertoires et des fichiers, ici un nœud peut contenir :
  - Des sous-domaines
  - des noms de machines

Représentation

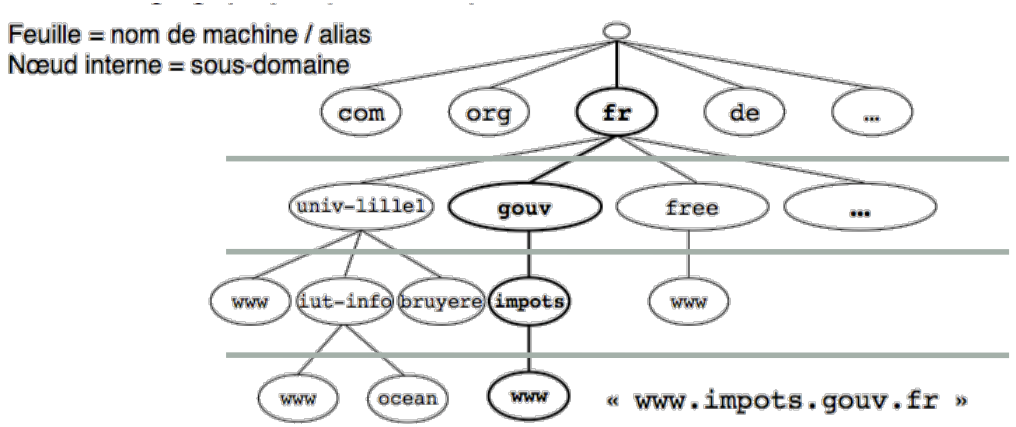
- La "descente" dans l'arbre est représentée dans une transcription textuelle de droite à gauche, chaque niveau de l'arborescence étant séparé du précédent par un point.



Délégation

- Le caractère distribué du système
  - Les nœuds pères délèguent aux nœuds fils la gestion
  - Un nœud père étant le nœud situé directement au dessus d'un ou plusieurs nœuds (ses nœuds fils)
- Lien entre un nœud père et un nœud fils
  - On définit au niveau du nœud père l'emplacement de la base de données de son nœud fils

Fr père de gouv
Gouv père de impots



Délégation

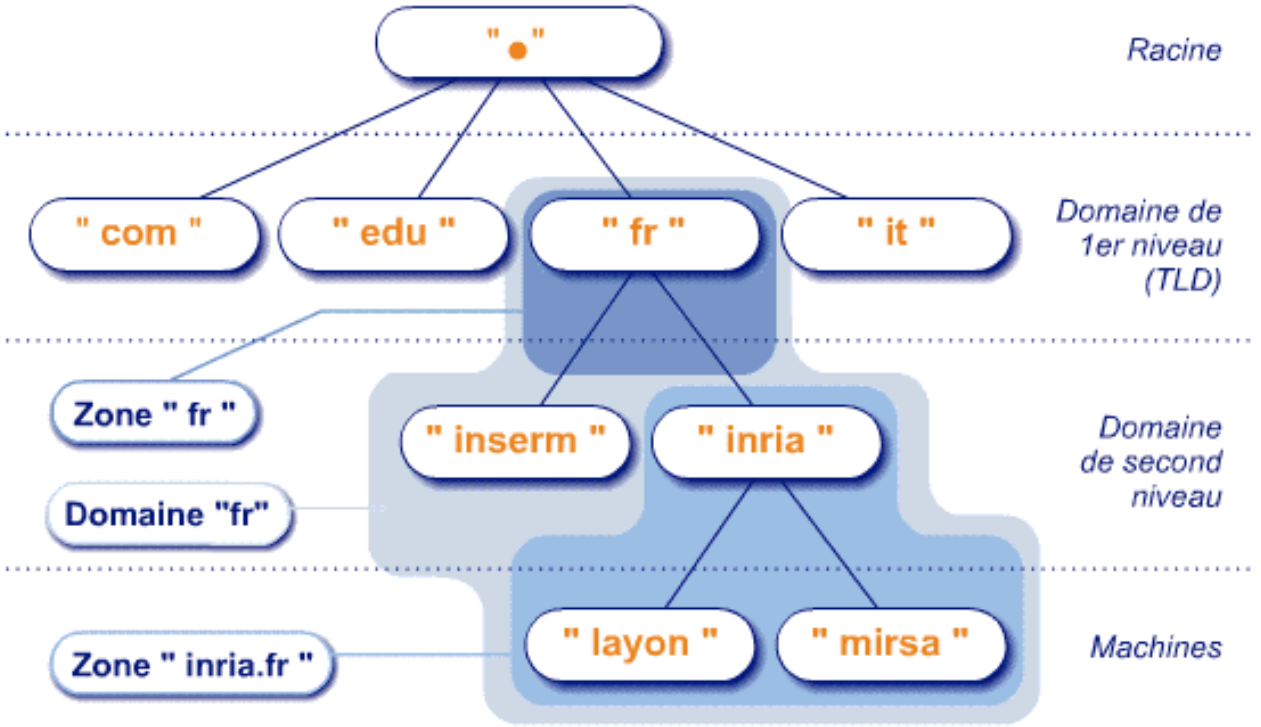
- Objectif
  - Distribuer la gestion du système entre les différents nœuds
  - Décentralisation "locale" pouvant aussi être opérée au niveau de chaque nœud
  - Création de domaines de responsabilité tout au long de l'arborescence
  - Délégations de gestion à chaque niveau

Nommage

- Un nom de domaine est obtenu par concaténation de labels de nœuds de l'arbre de nommage séparés par des points "."
- Les caractères autorisés pour les labels sont
  - "A ... Z",
  - "a ... z",
  - "0 ... 9",
  - "-";
- Aucune différence n'est faite entre les majuscules et minuscules
- Le label d'un nœud doit être unique pour le niveau dans lequel se situe le nœud
- La longueur maximale pour un label est de 63 caractères
- La longueur totale pour un nom de domaine est limitée à 255 caractères

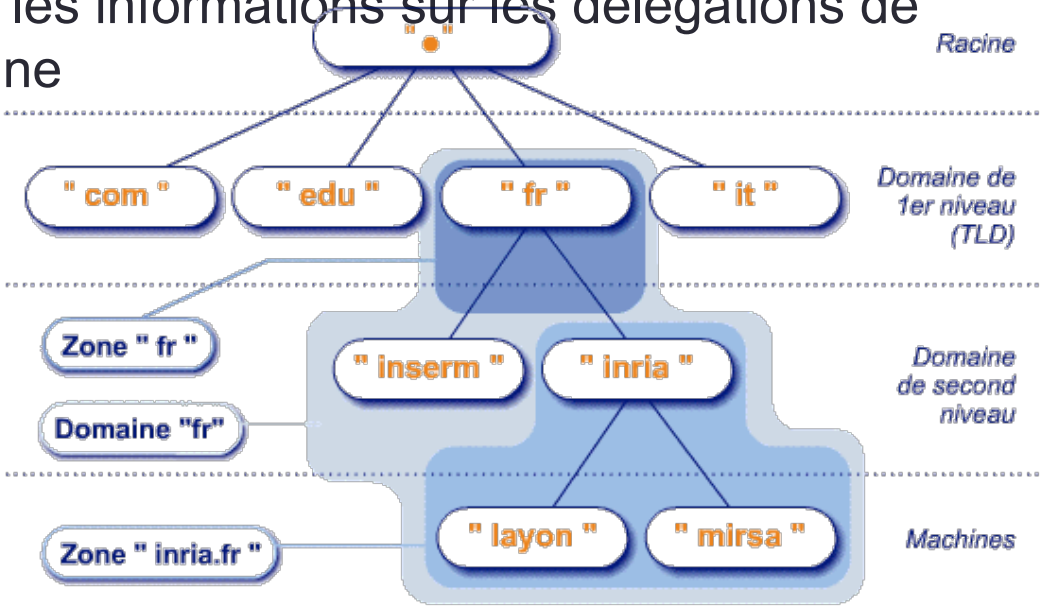
Domaine et zone

- Un domaine représente l'ensemble d'une sous-arborescence
  - Chaque noeud de l'arbre de nommage est un domaine
  - un sous- …es



Domaine et zone

- Une zone peut correspondre à un domaine, mais dans le cas général, il englobe uniquement une partie du domaine
  - le reste étant délégué à d'autres serveurs de noms
  - la zone "fr" est restreinte au noeud correspondant et contient notamment la partie descriptive du domaine sous la forme d'une base de données incluant les informations sur les délégations de gestion du reste du domaine



Architecture

- DNS fonctionne suivant le modèle client/serveur :
  - le client lance des requêtes DNS à travers une application spécialisée appelée resolve
  - Ces requêtes sont généralement adressées à un serveur de noms par défaut (par exemple le serveur de noms d'entreprise)
- Le service DNS est une application TCP/IP fonctionnant sur le port 53
  - s'appuie sur le service de transport UDP pour les requêtes et les réponses si taille < 512 octets
  - Sinon TCP (comme pour les opérations de transfert de zone entre serveurs de noms pour la mise à jour des répliqueurs)

Client

- Il existe 2 modes d'interrogation pour un résolver :
  - Le mode récursif :
    - le client (resolver) envoie une requête au serveur DNS
    - ce dernier renvoie une réponse complète au client qui est soit la correspondance recherchée soit un message d'erreur
    - Le serveur doit au besoin interroger d'autres serveurs de noms si le nom de domaine concerné par la requête n'est pas dans son cache et se trouve dans une zone pour laquelle il n'est pas autoritaire

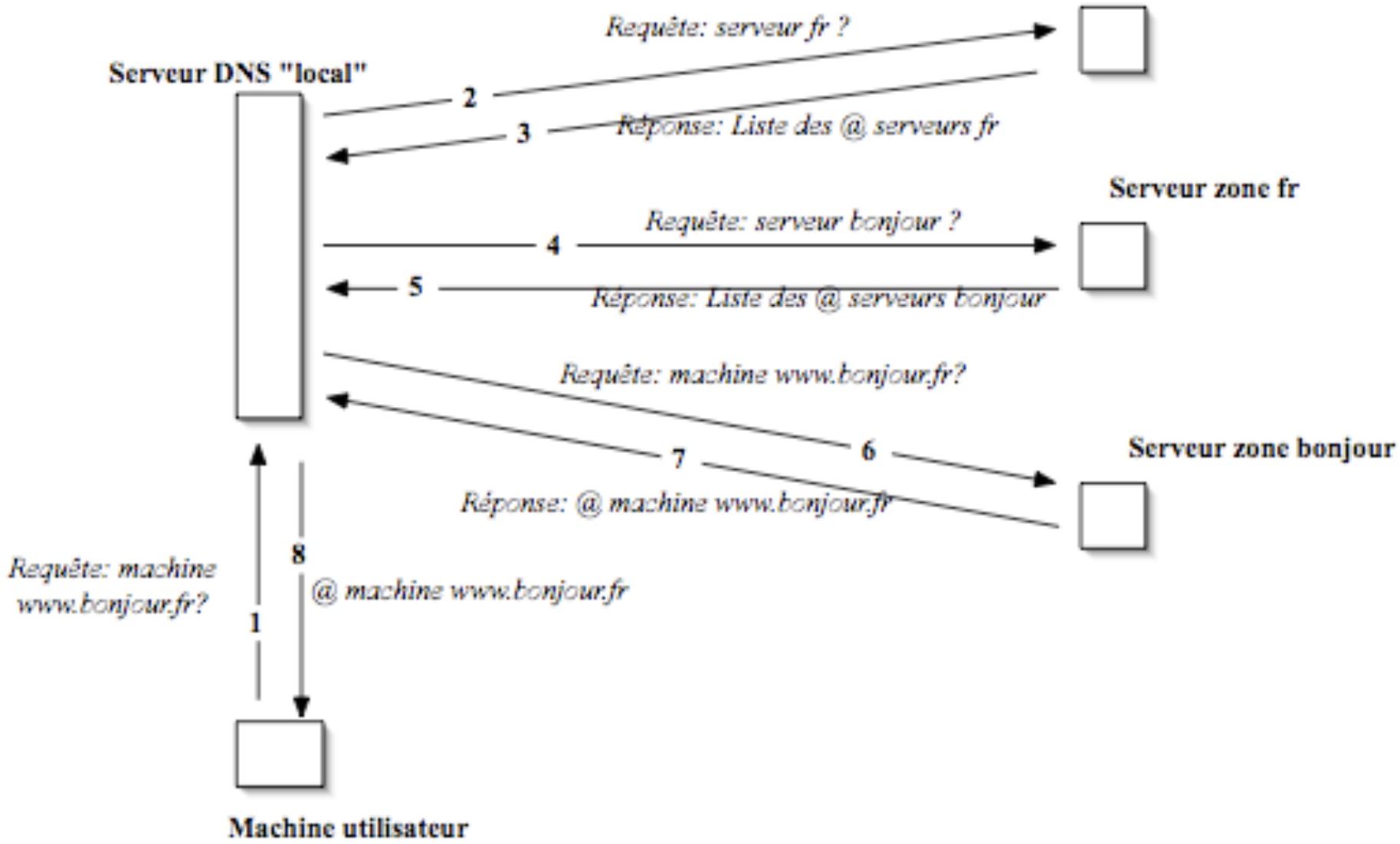
Client

- Il existe 2 modes d'interrogation pour un résolver :
  - Le mode non récursif ou itératif :
    - le client envoie une requête au serveur DNS ;
    - ce dernier renvoie soit la réponse complète (s'il est autoritaire pour la zone concernée) soit une réponse partielle (adresse d'un autre serveur de noms qui va permettre au client d'avancer dans le processus de résolution).
    - Le client va alors lancer une autre requête vers le serveur spécifié dans la réponse précédente.
    - Ce processus est répété autant de fois que nécessaire, permettant au client d'avancer à chaque requête d'un niveau dans l'arborescence qui mène vers le nom de domaine recherché.

Client

- En général
  - le mode récursif est utilisé par les applications clientes
  - le mode itératif par les resolvers des serveurs de noms
- Pour des raisons de performance et de sécurité, les administrateurs des serveurs de nom les configurent généralement pour qu'ils n'acceptent les requêtes en mode récursif que pour les machines de la zone pour laquelle ils sont autoritaires

Résolution

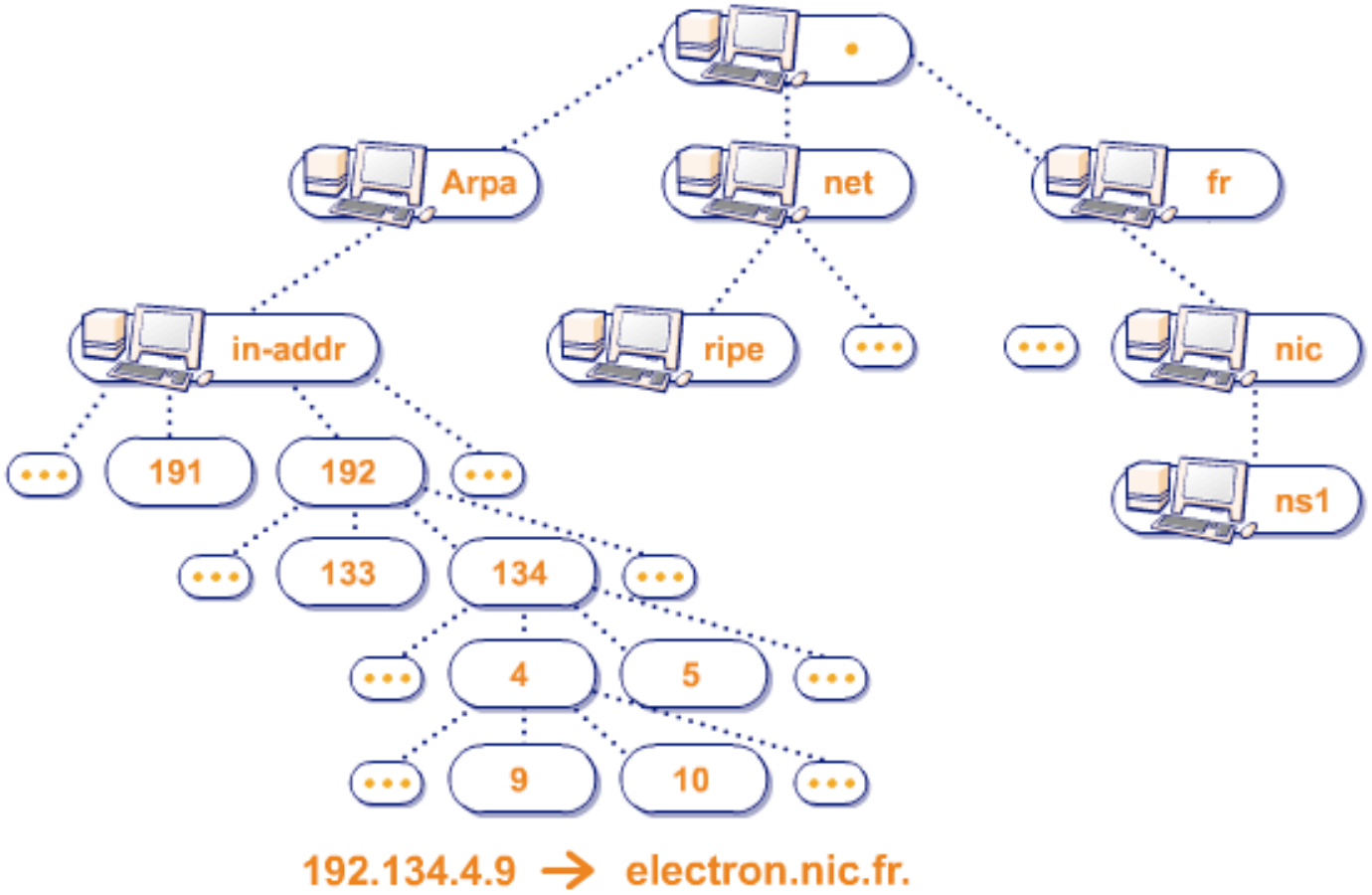

Requête: serveur fr ?
Serveur DNS "local"
2
3
Réponse: Liste des @ serveurs fr
Serveur zone fr
Requête: serveur bonjour ?
4
5
Réponse: Liste des @ serveurs bonjour
Requête: machine www.bonjour.fr?
6
7
Serveur zone bonjour
Réponse: @ machine www.bonjour.fr
Requête: machine www.bonjour.fr?
8
@ machine www.bonjour.fr
1
Machine utilisateur

Résolution inverse

- La résolution inverse consiste, à retrouver le nom d'une machine à partir de son adresse IP
  - s'appuie sur un système en arborescence qui part du domaine particulier in-addr.arpa, sous-domaine de arpa.
  - Dans l'arborescence pour la résolution inverse, chaque octet de l'adresse IP correspond à un niveau
  - pour chaque adresse, on crée un nom de domaine, sous-domaine de in-addr.arpa

Résolution inverse

Comment fait le DNS pour retrouver un nom de machine à partir d'une adresse IP ?



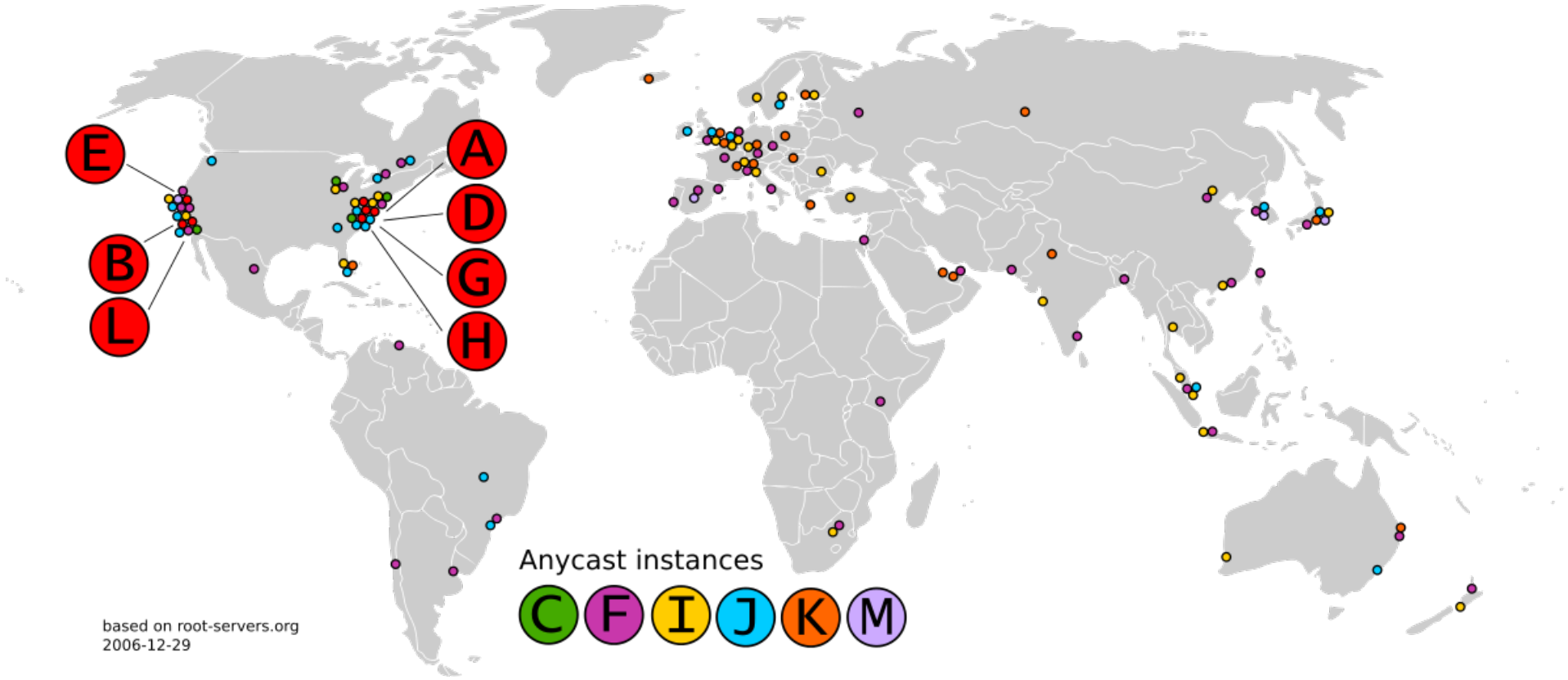
Serveurs racines

- La racine (root) occupe une place fondamentale dans l'arbre de nommage
  - Elle contient les références de tous les serveurs de domaines de premier niveau (TLD).
  - Importance primordiale pour le fonctionnement d'Internet
- Implémentation
  - réalisée à travers 13 serveurs répartis dans le monde
  - il y a ainsi plus de 130 sites dans 53 pays qui hébergent un serveur racine
  - système de réplication, contiennent la même information
- Serveurs root sont identifiés par les lettres de A à M et appartiennent tous au même domaine ROOT-SERVERS.NET

Serveurs racines

- A.ROOT-SERVERS.NET : VeriSign Global Registry Services
- B.ROOT-SERVERS.NET : Information Sciences Institute USC (USA)
- C.ROOT-SERVERS.NET : PSINet
- D.ROOT-SERVERS.NET : University of Maryland (USA)
- E.ROOT-SERVERS.NET : NASA Ames Research Center (USA)
- F.ROOT-SERVERS.NET : Internet Software Consortium (USA)
- G.ROOT-SERVERS.NET : U.S. DOD Network Information Center (USA)
- H.ROOT-SERVERS.NET : U.S. Army Research Lab (USA)
- I.ROOT-SERVERS.NET : NordU (Suède)
- J.ROOT-SERVERS.NET : VeriSign Global Registry Services (USA)
- K.ROOT-SERVERS.NET : RIPE NCC (UK, Europe)
- L.ROOT-SERVERS.NET : ICANN (USA)
- M.ROOT-SERVERS.NET : WIDE Project (Japon)

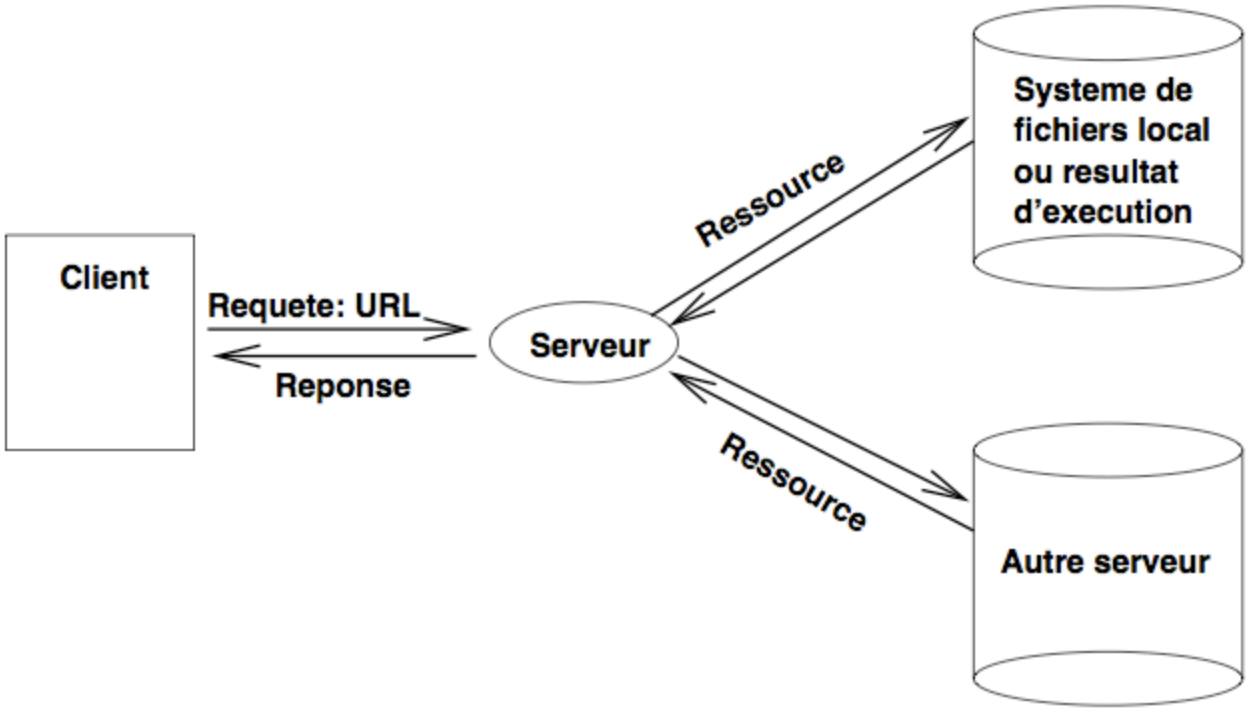
Localisation



HTTP

Introduction

- Base sur le principe du client / serveur
- Connexion en TCP/IP



HTTP

- Du point de vue du serveur
  - Statiques : HTML, texte, image, son
  - Dynamiques : SSI, CGI, php et autres scripts intégrés à l'HTML et interprétées par le serveur
- Du point de vue du client
  - Statiques : HTML, texte, images
  - Dynamiques : plug in ActiveX, Java, JavaScript

Version

- Versions
  - version 1.0 : la version initiale (RFC1945, mai 1996)
    - HEAD : permet de ne demander au serveur que l'en-tête, sans le document
    - GET: permet de demander une page
      - get <URI>
    - POST: permet d'envoyer des données au serveur
  - version 1.1 (RFC 2616 juin 1999)
    - OPTIONS : permet d'interroger le serveur sur les options disponibles.
    - TRACE : commande de débogage
    - Commandes désactivées
      - DELETE : permet de détruire un fichier sur le serveur
      - PUT : permet d'écrire des fichiers sur le serveur
  - Version 2 : RFC standard le 18 février 2015

Ressources

- URI : terme générique
  - Chaine de caractères identifiant de manière unique une resource sur l'internet
- En HTTP : on parle d'URL
  - Uniform Ressource Locator
  - Examples
  - http://<serveur>:<port>/<chemin absolue ressource>/<ressource>
  - http://<serveur>:<port>/<chemin absolue ressource>
  - http://<serveur>/<chemin absolue ressource>
  - http://<serveur>/<chemin absolue ressource>/<ressource>

Requête HTTP

- Ensemble de lignes envoyé au serveur par le navigateur
  - Une ligne pour la commande, l'URI, la version du protocole
  - Les champs d'en-tête de la requête
    - Des lignes facultatives pour donner des informations supplémentaires
  - Le corps de la requête
    - Des lignes optionnelles, séparées par une ligne vide et permettant un envoi de données (commande POST)
- exemple :

GET http://www.commentcamarche.net HTTP/1.0

Accept : text/html

If-Modified-Since : Saturday, 15-January-2000 14:37:11 GMT

User-Agent : Mozilla/4.0 (compatible; MSIE 5.0; Windows 95)

Commande

Commande	Description
GET	Requête de la ressource située à l'URL spécifiée
HEAD	Requête de l'en-tête de la ressource située à l'URL spécifiée
POST	Envoi de données au programme situé à l'URL spécifiée
PUT	Envoi de données à l'URL spécifiée
DELETE	Suppression de la ressource située à l'URL spécifiée

Réponse HTTP

- Un ensemble de lignes envoyées au navigateur par le serveur :
  - Une ligne de statut
    - La version du protocole utilisé
    - Le code de statut
    - La signification du code
  - Les champs d'en-tête de la réponse
    - ensemble de lignes facultatives permettant de donner des informations supplémentaires
    - lignes composée de : « nom » : « valeur »
  - Le corps de la réponse = le document demandé

Réponse HTTP, exemple

```
HTTP/1.0 200 OK
Date : Sat, 15 Jan 2000 14:37:12 GMT
Server : Microsoft-IIS/2.0
Content-Type : text/HTML
Content-Length : 1245
Last-Modified : Fri, 14 Jan 2000 08:25:13 GMT
... (le doc)
```

Réponse

Code	Message	Description
200	OK	La requête a été accomplie correctement
301	MOVED	Les données demandées ont été transférées à une nouvelle adresse
404	NOT FOUND	Classique! Le serveur n'a rien trouvé à l'adresse spécifiée. Parti sans laisser d'adresse... :)

FTP

Introduction

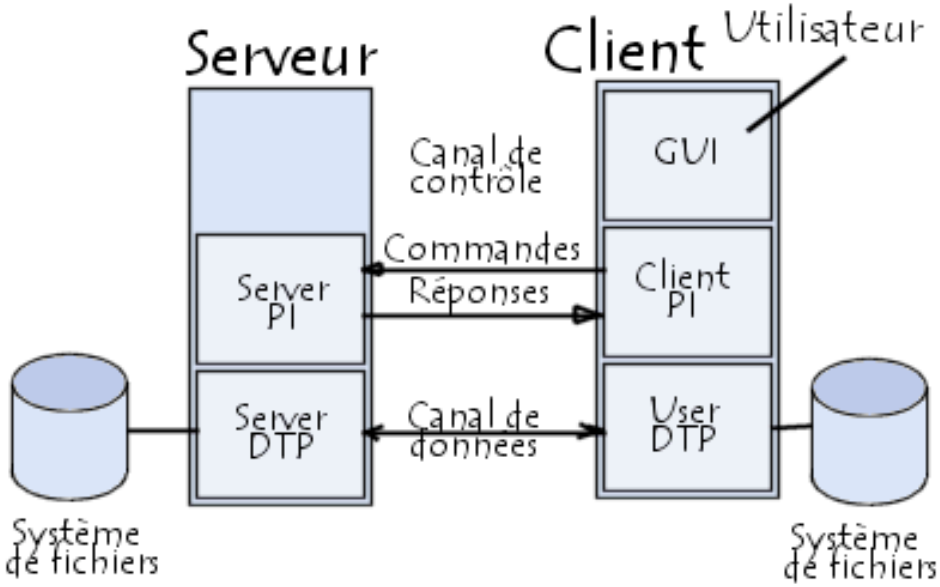
- Le protocole FTP (File Transfer Protocol) est un protocole de transfert de fichier.
- La mise en place du protocole FTP date de 1971 :
  - RFC 141
  - actuellement défini par le RFC 959

Rôle

- Le protocole FTP définit une façon de transférer des données sur un réseau TCP/IP.
- Le protocole FTP a pour objectifs de :
  - permettre un partage de fichiers entre machines distantes
  - permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
  - permettre de transférer des données de manière efficace

Modèle

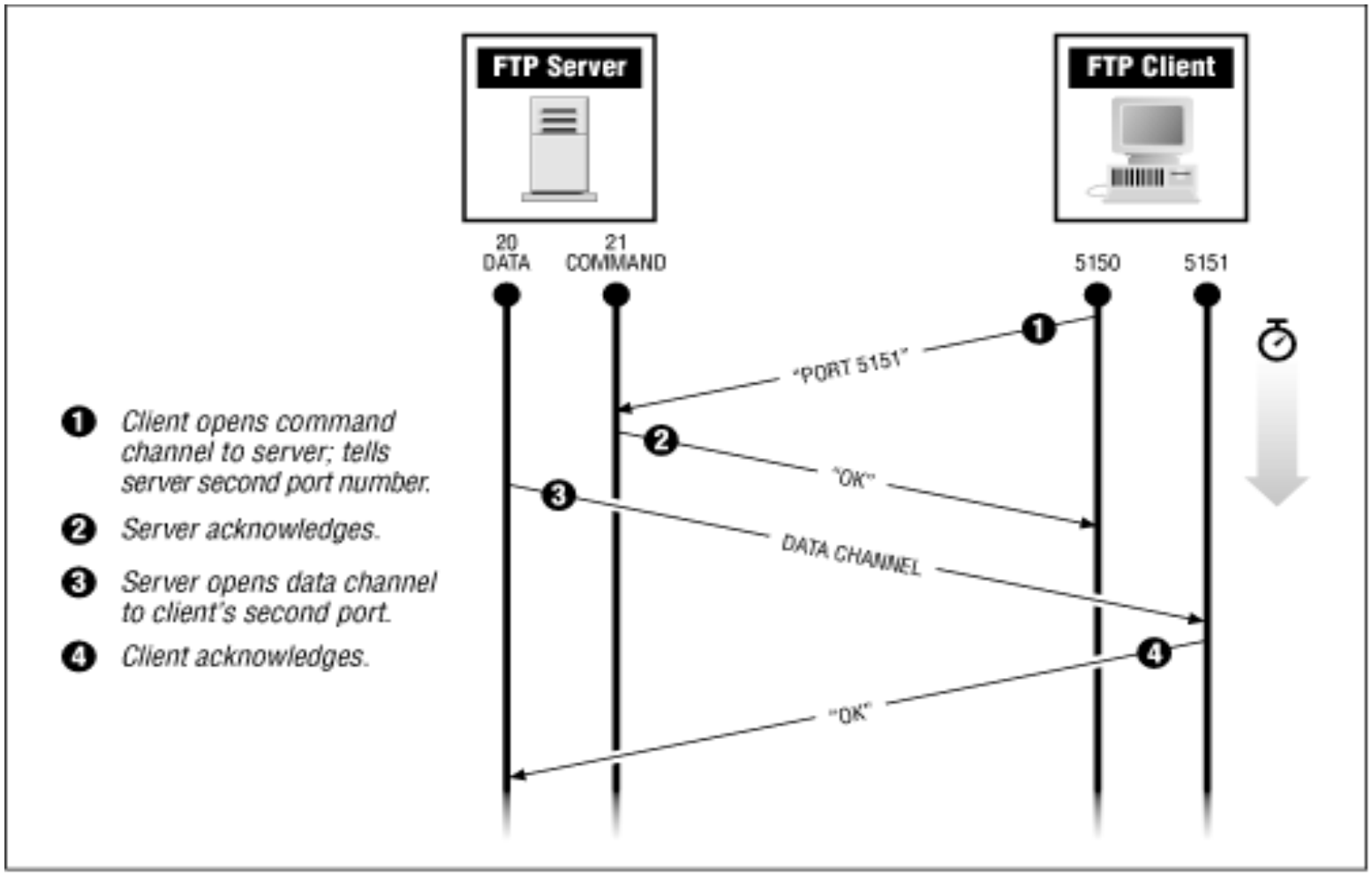
- Modèle client-serveur
- Lors d'une connexion FTP, deux canaux de transmission sont ouverts :
  - Un canal pour les commandes (canal de contrôle)
  - Un canal pour les données



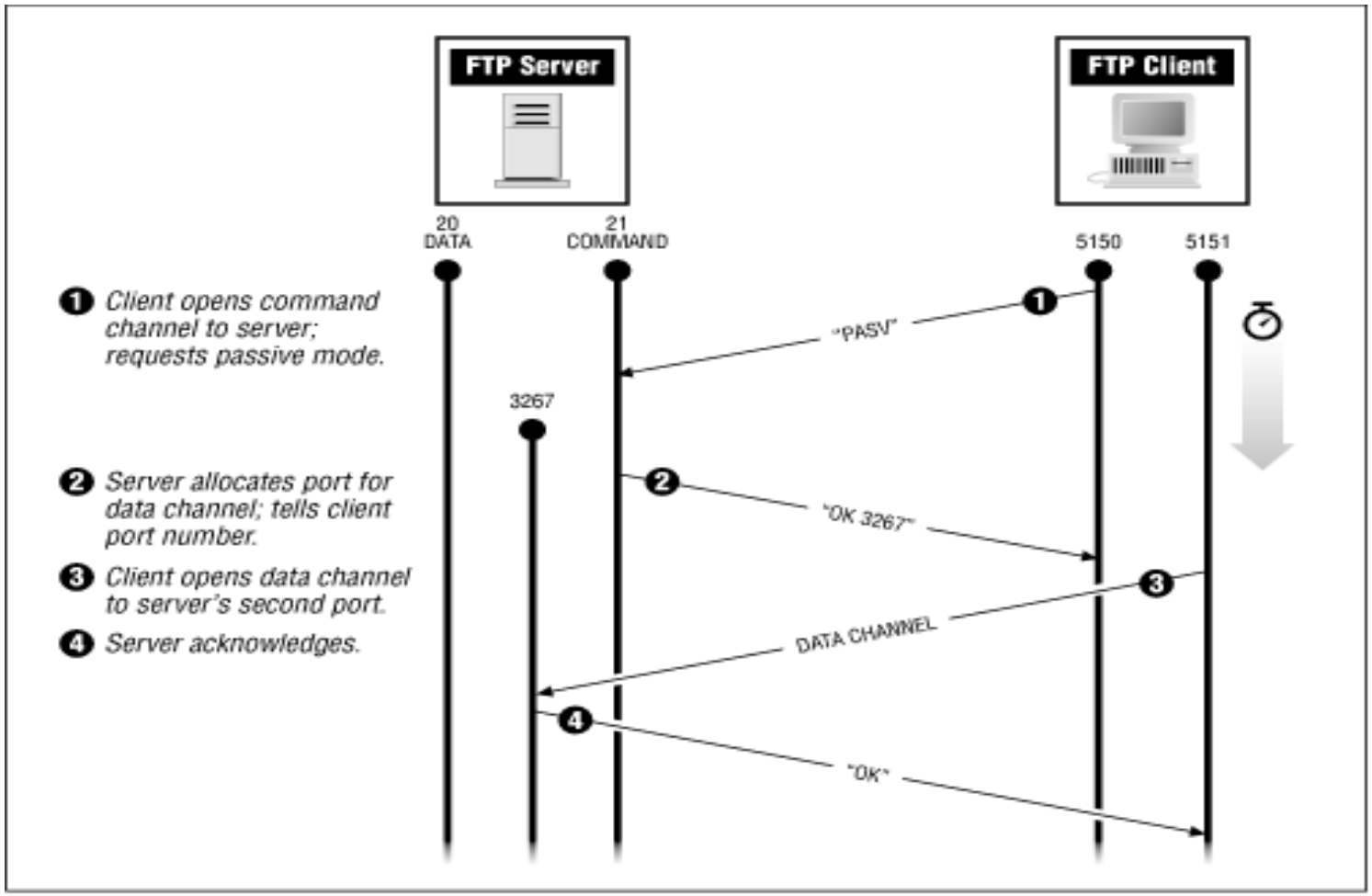
Rôle

- Le client et le serveur possèdent deux processus permettant de gérer :
  - le DTP (Data Transfer Process) chargé
    - d'établir la connexion,
    - de gérer le canal de données.
  - le PI (Protocol Interpreter)
    - permet de commander le DTP à l'aide de commandes reçues sur le canal de contrôle.
    - Coté serveur :
      - écouter les commandes provenant d'un client
      - Y répondre
      - d'établir la connexion pour le canal de contrôle
    - Coté client :
      - établir la connexion avec le serveur FTP
      - envoyer les commandes FTP, de recevoir les réponses serveur

FTP mode actif



FTP mode passif



Commande de contrôle

Commande de contrôle d'accès	
Commande	**Description**
USER	Chaîne de caractères permettant d'identifier l'utilisateur. L'identification de l'utilisateur est nécessaire pour établir une communication sur le canal de données
PASS	Chaîne de caractères spécifiant le mot de passe de l'utilisateur. Cette commande doit être immédiatement précédée de la commande *USER*. Il revient au client de masquer l'affichage de cette commande pour des raisons de sécurité
ACCT	Chaîne de caractères représentant le compte (account) de l'utilisateur. Cette commande n'est généralement pas nécessaire. Lors de la réponse à l'acceptation du mot de passe, si la réponse est 230 cette phase n'est pas nécessaire, si la réponse est 332, elle l'est
CWD	*Change Working Directory* : cette commande permet de changer le répertoire courant. Cette commande nécessite le chemin d'accès au répertoire à atteindre comme argument
CDUP	*Change to Parent Directory* : cette commande permet de remonter au répertoire parent. Elle a été introduite pour remédier aux problèmes de nommage de répertoire parent selon les système (généralement "..")
SMNT	*Structure Mount* :
REIN	*Reinitialize* :
QUIT	Commande permettant de terminer la session en cours. Le serveur attend de finir le transfert en cours le cas échéant, puis de fournir une réponse avant de fermer la connexion

Commande de service

Commande de service FTP	
Commande	**Description**
RETR	Cette commande (*RETRIEVE*) demande au serveur DTP une copie du fichier dont le chemin d'accès est passé en paramètre.
STOR	Cette commande (*store*) demande au serveur DTP d'accepter les données envoyées sur le canal de données et de les stocker dans le fichier portant le nom passé en paramètre. Si le fichier n'existe pas, le serveur le crée, sinon il l'écrase
DELE	Cette commande (*delete*) permet de supprimer le fichier dont le nom est passé en paramètre. Cette commande est irrémédiable, seule une confirmation au niveau du client peut être faite.
RMD	Cette commande (*remove directory*) permet de supprimer un répertoire. Elle indique en paramètre le nom du répertoire à supprimer
MKD	Cette commande (*make directory*) permet de créer un répertoire. Elle indique en paramètre le nom du répertoire à créer
PWD	Cette commande (*print working directory*) permet de renvoyer le chemin complet du répertoire courant
LIST	Cette commande permet de renvoyer la liste des fichiers et répertoires présents dans le répertoire courant. Cette liste est envoyée sur le DTP passif. Il est possible de passer en paramètre de cette commande un nom de répertoire, le serveur DTP enverra la liste des fichiers dans le répertoire passé en paramètre

Utilisation

- D'abord, pour se connecter au serveur, il faut taper :
  - `ftp ftpperso.free.fr`
- Ensuite, on vous demande votre login :
  - `User : [votre_login]`
- Puis votre mot de passe :
  - `Password: [votre_mot_de_passe]`
- Vous arrivez alors sur la ligne suivante :
  - `ftp>`

Cette ligne représente le prompt de la connexion ftp.

Utilisation : **connexion en anonyme**

- Sur certains sites, il est possible de se connecter en **anonymous**, sans login.
  - permettre les téléchargement
  - mais pas de dépots.
- Le login est "anonymous",
- Le mot de passe est une adresse mail

Utilisation : lister

- Afficher le contenu du répertoire

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
mysql
index.html
226-Transfer complete.
226 Quotas on: using 13440.00 of 104857600.00 bytes
ftp : 401 octets reçus en 0,03 secondes à 13,37 Ko/sec.
```

Utilisation : **Navigation**

- Navigation sur le serveur distant

```
ftp> cd images
250 CWD command successful.
```

- Navigation sur le disque local

```
ftp> lcd  /
```

- Création de répertoire

```
ftp> mkdir images
```

Utilisation : transfert

- Envoi de fichiers

```
ftp> bin
ftp> hash
ftp> put index.html
ftp> mput *.gif
```

- Téléchargement

```
ftp> getindex.html
ftp> mget *.gif
```

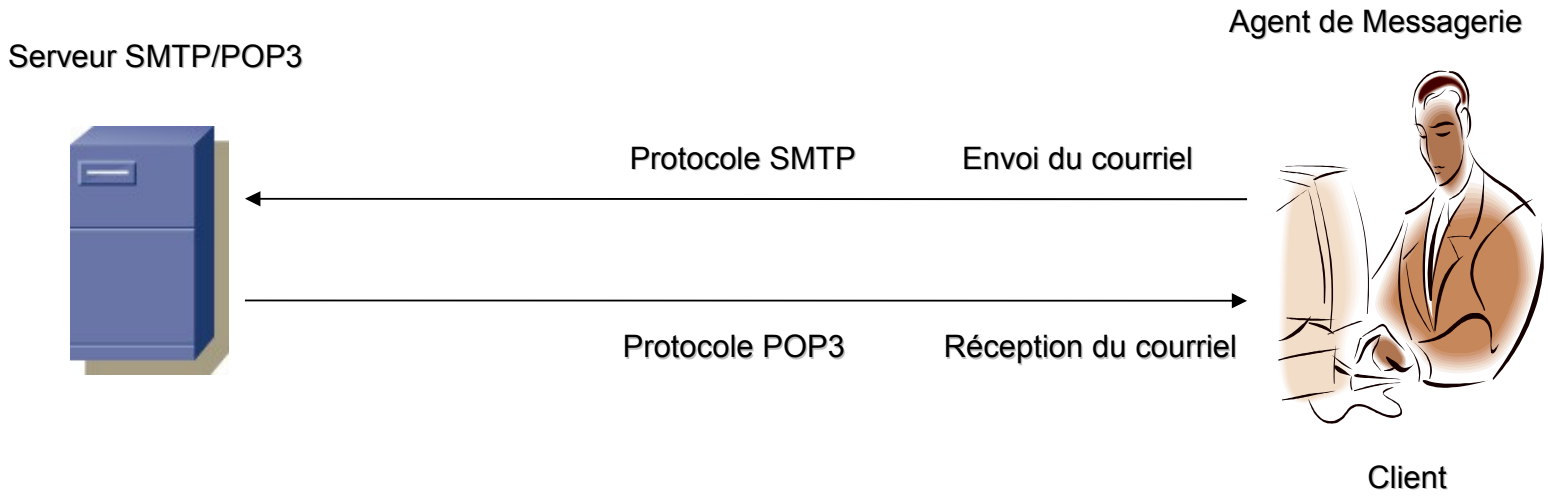
Utilisation : fermeture

- Fermeture de la connexion
  - Close
  - Quit
  - Open

- Utilisation d’un navigateur web
  - ftp://toto@machine.fr

SMTP

Courrier


Agent de Messagerie
Serveur SMTP/POP3
Protocole SMTP
Envoi du courriel
Protocole POP3
Réception du courriel
Client

Intoduction

- Proposé en 1982,
- **SMTP** (*Simple Mail Transfer Protocol*)
  - Proposé en 1982 → RFC 821,
  - 1990 : RFC 2554 (authentification), RFC 2476
  - 2008 : RFC 5321 (courrier mobile)
- *But :*
  - *transporter* les messages sur les différents réseaux (TCP/IP ou l'autres réseaux)
- Fonction en client /serveur

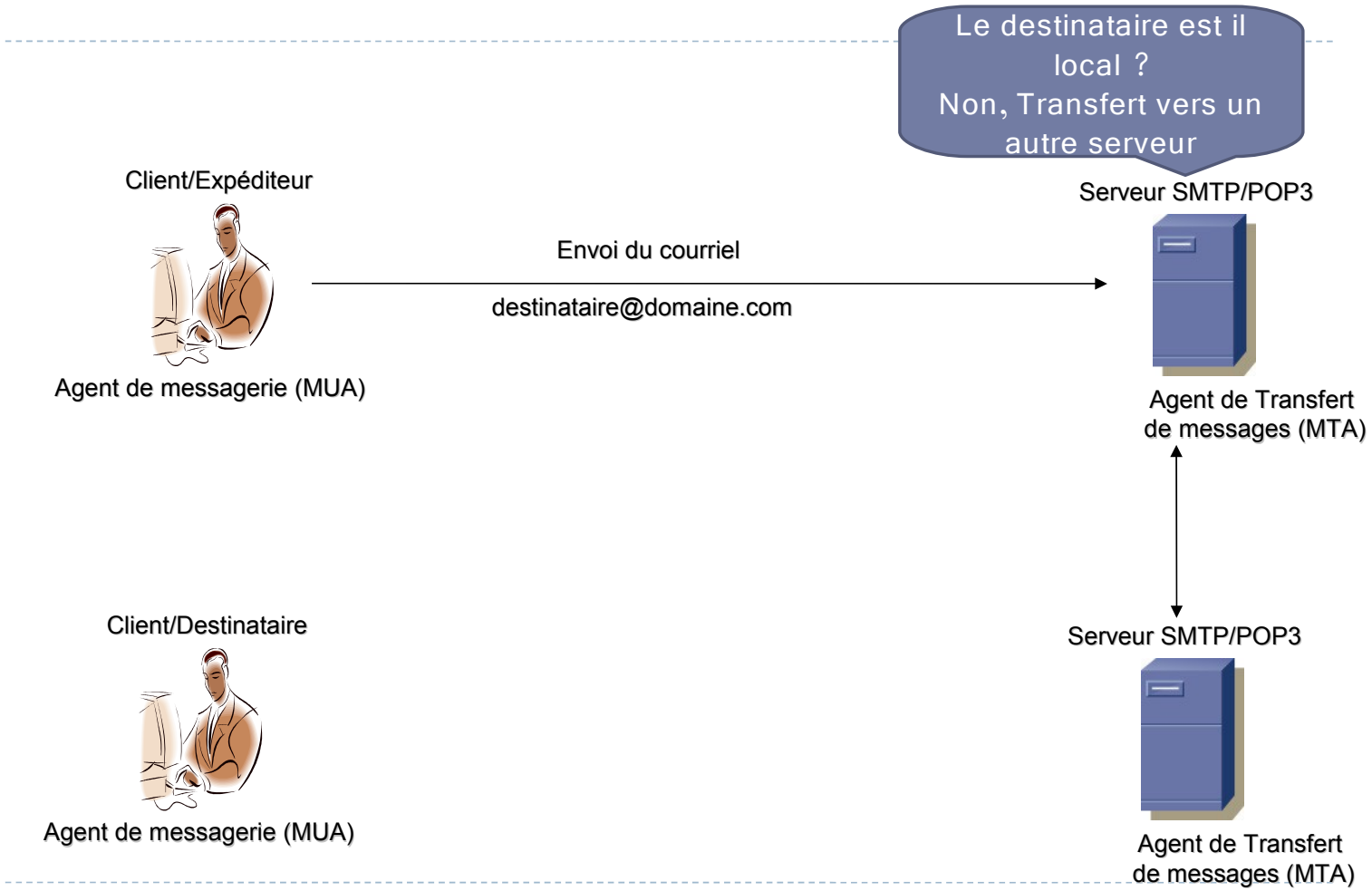
Modèle

- Acteurs :
  - MUA : Mail User Agent = client de messagerie qui envoie au MSA
  - MSA : Mail Soumission Agent = un serveur de messagerie émetteur (relai) qui transfère au MTA
  - MTA : Mail Transfer Agent = un serveur de messagerie émetteur (commutateur) qui envoie le message au MX destinataire
  - MX : Mail exchanger = le serveur de messagerie destinataire
  - MDA : Mail delivery agent = le serveur de messagerie destinataire qui délivre

Principe : envoyer

- **MUA** (*Mail User Agent*) soumet le courrier au serveur MSA en passant par SMTP/TCP port *587 (avec authentification) ou port 465 (SSL)* ou port *25* (historique)
- **MSA** *(Mail Soumission Agent)* transfère le courrier au MTA
- **MTA** *(Mail Transfer Agent)*
  - recherche d'abord la localisation du destinataire du courrier en interrogeant le DNS (*type* MX) puis recherche l'IP
  - Puis se connecte au serveur du destinataire comme un client SMTP
- **MX** (*Mail Exchanger*) accepte le courrier et le transmet à MDA
- **MDA** (*Mail Delivery Agent*)
  - Il enregistre les courriers en format *mailbox*

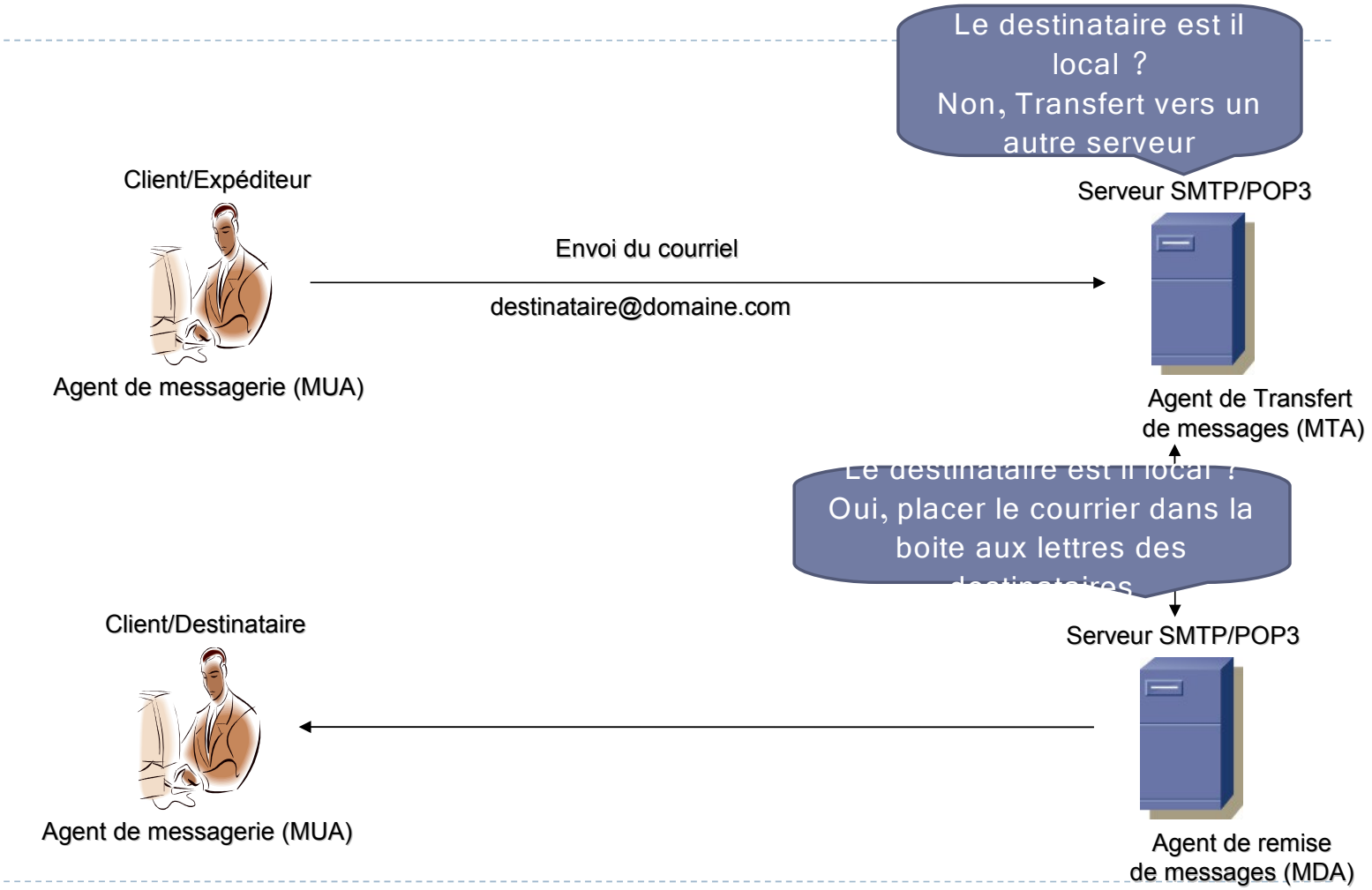
illustration



Principe : recevoir

- Il existe plusieurs protocoles de client :
  - POP (*Post Office Protocol*)
  - IMAP *(Internet Message Access Protocol)*
  - + système propriétaire (exchange)
- Le client (MUA) doit *s'authentifier* pour retirer ses courriers stockés sur le serveur local

illustration



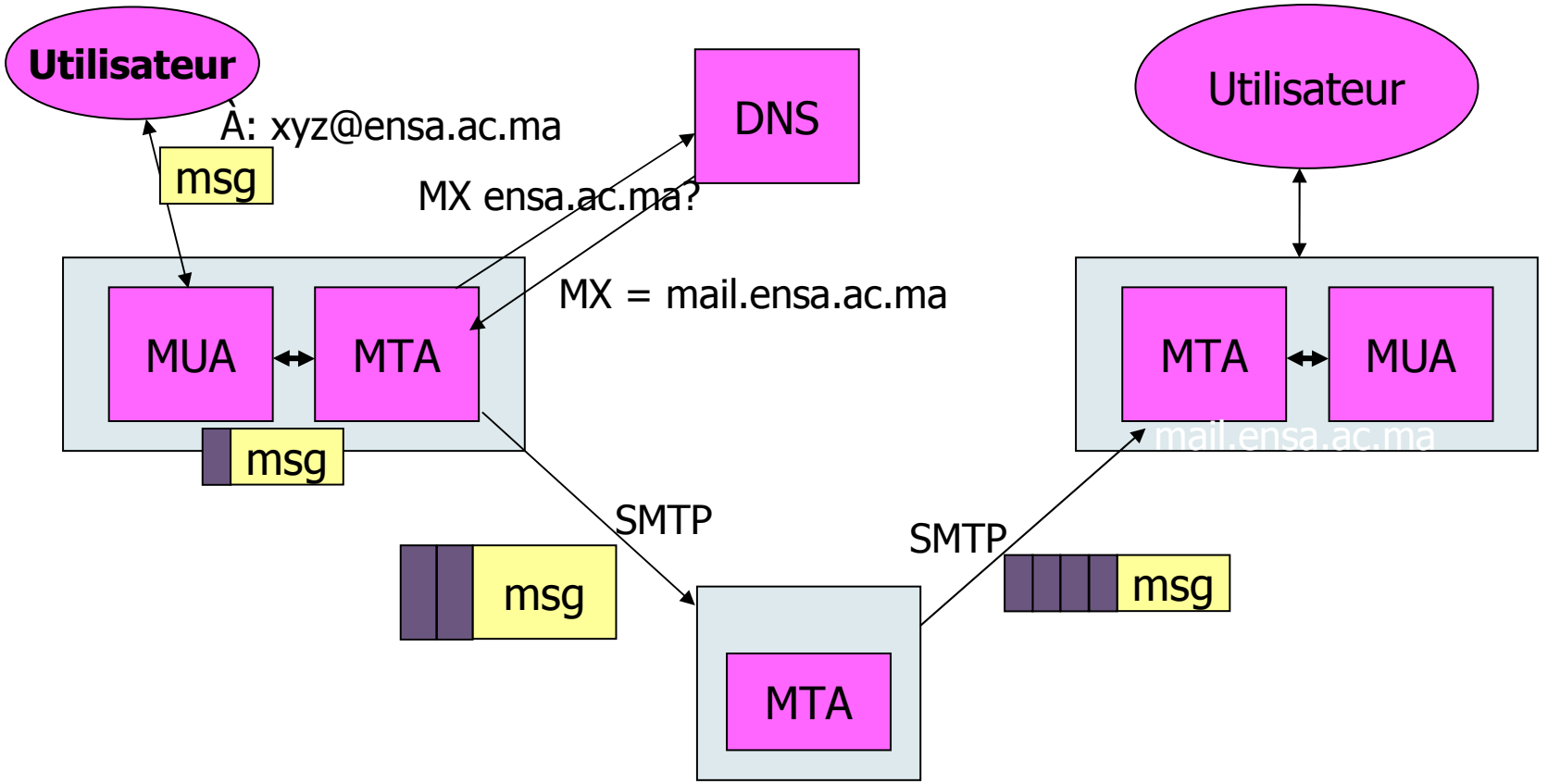
Adresse

- Les adresses mail : RFC 5321 et 5322
  - 2 parties : le nom de boîte à lettre et le nom de domaine DNS
  - Exemple : sylvain.meignier@univ-lemans.fr
  - Le nom
    - ne doit pas dépasser 64 octets
    - il n’est pas attaché au login
  - Le nom de domaine est déterminé par l'entré MX du domaine

SMTP principales commandes client

- Chaque requête (un message du protocole SMTP) correspond à une ligne de texte terminée par CRLF
- **HELO** <SP> <domaine> <CRLF>
  - ouverture de session entre le client et le serveur (le message contient le nom de domaine FQDN du client).
- **MAIL** <SP> FROM: <route-retour> <CRLF>
  - Définit l'adresse mail de l'émetteur (utilisé pour le retour éventuel d'erreurs).
- **RCPT** <SP> TO: <route-aller> <CRLF**>**
  - Définit l'adresse d'un
- **DATA** <CRLF>
  - Définit l'enveloppe (l'entête) et le corps (le texte) du message.
- **QUIT** <CRLF>
  - Termine un courrier.

Principe


Utilisateur
A: xyz@ensa.ac.ma
msg
DNS
MX ensa.ac.ma?
MX = mail.ensa.ac.ma
MUA
MTA
msg
Utilisateur
MTA
MUA
mail.ensa.ac.ma
SMTP
SMTP
msg
msg
MTA

POP ET IMAP

POP

- Le protocole POP3 (*Post Office Protocol version 3*)
  - RFC 1939, port 110
- est largement implémenté
- Le principe :
  - un client connecte au serveur pour *relever définitivement* les messages
  - les messages sont transmis vers le client
- Le client doit *s'authentifier*
  - *Par défaut mot de passe en claire*
  - Ou TLS (Transport Layer Security) et SSL (Secure Socket Layer)

POP : Commandes

- USER : Fourniture du nom de la boite aux lettres
- PASS : Fourniture du mot de passe en clair
- STAT : Nombre de messages dans la boite
- RETR : Transfert du message *n*
- DELE : Marquage message pour la suppression
- QUIT : Fin de session.

IMAP

- Le protocole IMAP4 (*Internet Message Access Protocol*),
- RFC 2060 → 3501 qui remplace le RFC 2060, port 143
- Protocole le plus complet que POP
- Le principe
  - deux modes : connecté et déconnecté *disconnected modes*)
  - permettent à un client de connecter (ou déconnecter, les courriers récupérés durant une connexion sont dans un cache) au serveur pour *relever* les messages en attente
  - les messages souvent restent dans la boîte aux lettres sur le serveur de messagerie
    - → permet de consulter ses courriers avec plusieurs machines/clients

IMAP : Commandes

- **AUTHENTICATE** : Mécanisme d'authentification choisi.
- **LOGIN** : Usager mot de passe.
- **LOGOUT :** Fin de session IMAP.
- **CREATE/DELETE/RENAME** : Nom de boite aux lettres.
- **SELECT/EXAMINE** : Nom de boite aux lettres.
- **LIST/LSUB/STATUS** : Etat de boite aux lettres.
- **EXPUNGE/CLOSE** : Détruit les messages marqués (et ferme).
- **SEARCH** : Recherche de message sur différents critères.
- **FETCH** : Récupération des données concernant un courrier.
- **COPY** : Recopie d'un message d 'une boite aux lettres dans une autre.
- **CAPABILITY** : Liste des fonctions implantées d'un serveur.
- **NOOP :** Opération vide.

DHCP

Source : http://irt.enseeiht.fr/anas/cours/6Sces.pdf

Service DHCP

- Sur les réseaux locaux de grande taille ou sur les réseaux dont les utilisateurs changent fréquemment, le
- service DHCP est très recommandé.
  - De nouveaux utilisateurs peuvent se présenter travaillant sur des ordinateurs portables et nécessitant une connexion.
  - D'autres peuvent disposer de nouvelles stations de travail devant être connectées.
  - Plutôt que de faire attribuer des adresses IP par l'administrateur réseau à chaque station de travail, il est plus efficace que les adresses IP soient attribuées automatiquement à l'aide du protocole DHCP.

Protocole

- **DHCP : Dynamic Host Configuration Protocol**
  - Protocole de configuration Dynamique des clients
- DHCP est une extension de BOOTP
  - permet à un client sans disque dur de démarrer et de configurer automatiquement TCP/IP.
- Permettre à un client d'obtenir dynamiquement une adresse IP (et d'autres paramètres éventuellement) auprès d'un serveur DHCP.
  - Automatiser l'affectation des adresses IP, des masques de sous-réseau, des paramètres de passerelle …
- Remarques:
  - *Un réseau peut avoir plusieurs serveurs DHCP.*
  - *Le client ne désigne pas un serveur*

- Le serveur DHCP est contacté et une adresse est demandée.
- Le serveur DHCP :
  - choisit une adresse dans une plage d’adresses configurée nommée pool
    - les adresses qui ne sont plus utilisées sont automatiquement remises dans le pool pour être réattribuées.
  - attribue temporairement une adresse au client DHCP pour une durée définie nommée Bail.

DHCP : demande

- L'obtention d'une adresse se fait en 4 phases :
  - Demande de bail IP par le client.
  - Offre de bail IP par un serveur.
  - Sélection d'une offre par le client.
  - Accusé de réception de bail IP par le serveur.

Demande : client

- Lorsqu'un périphérique, configuré pour le protocole DHCP, est mis sous tension ou se connecte au réseau diffuse une demande d'adresse IP (*DhcpDiscover*) avec :
  - **source 0.0.0.0**
  - **destination 255.255.255.255**
  - **Adresse MAC client**
- Le client DHCP attend une offre pendant une seconde
- En cas de non réponse il rediffuse sa demande quatre fois (à des intervalle de 9, 13 et 16 secondes puis un intervalle aléatoire entre 0 et 1000 millisecondes).
- Après ces quatre tentatives, il renouvelle sa demande toutes les 5 minutes.

Offre de bail

- Tous les serveurs reçoivent la demande.

- S'ils sont configurés pour répondre, ils diffusent des offres (*DhcpOffer*) avec les informations suivantes :
  - L'adresse MAC du client
  - Une adresse IP
  - Un masque de sous-réseau
  - Une durée de bail (durée pendant laquelle l'IP ne sera pas utilisée par un autre host)
  - Son adresse IP (du serveur)

Sélection de l'offre

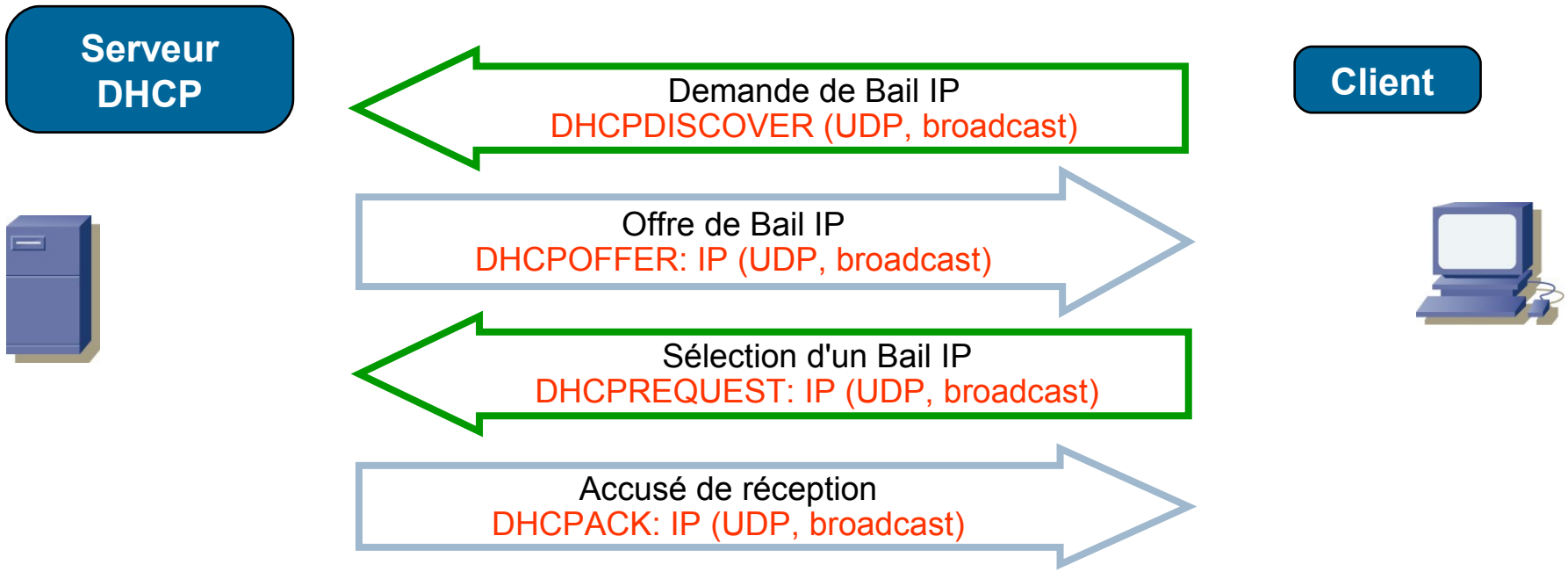
- Le client sélectionne une offre (en général la première)
- Le client annonce par diffusion qu'il a accepté une offre (***DhcpRequest***).
- Le message ***DhcpRequest*** comporte l'identification du serveur sélectionné
- Ce dernier sait que son offre a été retenue
- Tous les autres serveurs DHCP retirent leurs offres

ACK

- Le serveur ainsi sélectionné envoi accusé de réception au client (***DhcpAck***).
- Son message contient éventuellement d'autres informations (serveur DNS, Passerelle, etc.)

Résumé

- UDP, port 68



Principaux paramètres

- RFC 2132 précise les principaux paramètres pouvant être affectés par DHCP, notamment :
  - **Un masque de sous-réseau**
  - **L'adresse IP du serveur DNS et le nom de domaine dans lequel est situé la station**
  - **Le nom de la station**
  - **L'adresse IP du serveur WINS et le type de nœud Netbios**
  - **Des paramètres IP, TCP, ARP tels que MTU, TTL, la durée du cache ARP,**
  - **Des routes statiques par défaut ainsi que l'adresse du routeur par défaut**
  - **Les serveurs de messagerie SMTP et POP**
  - **Divers serveurs par défaut tels que Web, News, NTP, ...**
  - **Des paramètres relatifs au DHCP tel que le bail**
  - **Les types de messages DHCP (Discover, Request, Release, ...)**
  - **...**
- Les options sont au nombre de 65 recensées à ce jour

Renouvellement

- L'affectation d'une adresse IP n'est pas permanente, elle est accordée pour une durée limitée qui est le bail
  - Une fois que le client obtient le bail, celui-ci doit être renouvelé avant son expiration via un autre message DHCP REQUEST.
  - Le client doit donc renouveler ce bail
- Deux modes de renouvellement possibles :
  - **1. Automatique(Timetriggred)**
  - **2. Manuel(utilisateur)**

Renouvellement

- 1ère demande de renouvellement
  - à 50% de l'utilisation du bail, le client envoie un message DHCPREQUEST pour le renouvellement de son bail.
  - Si elle est accordée, le client continue avec un nouveau bail et éventuellement de nouveaux paramètres (*DhcpAck*).
  - Si le serveur est absent, le bail reste donc valide pendant 50% de la valeur initiale

Renouvellement

- 2ème demande de renouvellement
  - à 87.5% du bail, si le serveur est indisponible, le client envoie un message DHCPDISCOVER.
  - Cette fois la demande est adressée à tous les serveurs (diffusion).
    - Un serveur peut répondre en proposant un nouveau bail (*DhcpAck*)
    - Mais peut également répondre avec un message *DhcpNack* qui oblige le client à se réinitialiser (reprise de la procédure d'obtention d'un bail)
- **Si le bail expire (ou *message DhcpNack*)**
  - À 100% du bail : reprise de la procédure, normale, d'obtention d'un bail

Messages

- **DHCPDISCOVER :** Requête de Localisation des serveurs DHCP disponibles **DHCPOFFER :** Réponse d'un serveur à un paquet DHCPDISCOVER, contenant les premiers paramètres DHCP
- **DHCPREQUEST :** Requête du client pour annoncer qu'il a accepté une offre ou pour prolonger son bail
- **DHCPACK :** Réponse du serveur contenant des paramètres supplémentaires en plus de l'adresse IP du client
- **DHCPNAK :** Réponse du serveur pour signaler au client que son bail est expiré ou si le client annonce une mauvaise configuration réseau
- **DHCPDECLINE :** le client annonce au serveur que l'adresse est déjà utilisée **DHCPRELEASE :** le client libère son adresse IP
- **DHCPINFORM :** le client demande des paramètres locaux de configuration si il a obtenu une adresse réseau grâce à d'autres moyens (ex. configuration manuelle)

Serveur

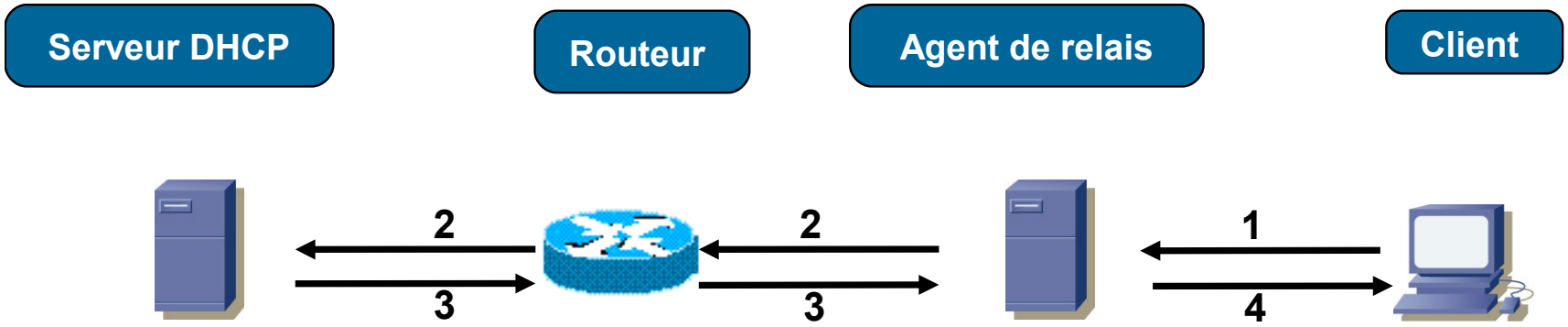
- Nous pouvons utiliser un routeur comme un serveur DHCP
- L' exemple suivant montre une configuration de routeur Cisco comme un serveur DHCP dans le réseau 192.168.1.0/24.
  - *conf t*
    service dhcp
    ip dhcp pool 192.168.1.0/24
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
    dns-server 192.168.1.5 192.168.1.6
    exit
    ip dhcp excluded-address 192.168.1.1 192.168.1.199
    ip dhcp excluded-address 192.168.1.241 192.168.1.255
- Avec les adresses exclus, uniquement les adresses IP entre 192.168.1.200-192.168.1.240 seront disponibles pour les clients.

Sergmentation du réseau

- Les trames brodcast ne traversent pas les routeurs.
- Sur un réseau segmenté par des routeurs il est donc impossible de servir tous les segments avec le même serveur DHCP.
  - ***Il faut donc mettre un serveur DHCP sur chaque segment,***
  - ***Ou utiliser un agent de relais DHCP.***
- **Un agent de relais DHCP relaye** les messages DHCP échangés entre un client et un serveur DHCP situés sur des sous-réseaux différents.
  - Il est généralement installé sur un routeur pour pouvoir diriger les messages vers le serveur DHCP.
  - L'agent doit connaître l'adresse du serveur DHCP mais ne peut pas être lui- même client DHCP.
- Serveur DHCP et agent de relais ont des adresses ip statiques.
- **Le dialogue traverse le routeur et se fait en unicast.**

Relais DHCP

- Le client envoie une trame de broadcast DhcpDiscover (1)
- l'agent de relais transfère la requête à la liste des serveurs DHCP spécifiés lors du configuration de l'agent (2).
- Le serveur retourne à l'agent une adresse (3)
- L'agent diffuse la réponse sur le réseau ayant envoyé la requête d'origine (4).



Attribution des adresses

- 2 modes :
  - Dynamique : les adresses attribuées via le DHCP ne sont pas affectées aux hôtes définitivement.
    - Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée.
  - Fixe déterminer en fonction de l'adresse MAC des machines

SSH