Thème n°4 : Les Applicatifs Réseaux

Le Service de Noms de l'Internet:

DNS

(Domain Name System)

Laurence Duchien

UV B: Complément Réseaux de Transport et Applications

Année 95/96

Laurence Duchien

CNAM-Cedric, 292, rue st Martin
75141 Paris Cedex 03
tel : 40 27 25 83
e_mail : duchien@cnam.fr
http://tulipe.cnam.fr/personne/duchien/poly.html

Plan

1. L'Internet..... 3
Quelques Caractéristiques..... 4
Type d'utilisation 5
Les Moyens..... 6
2. Le problème de la résolution de noms en adresse 7
3. La Désignation Universelle..... 8
3. La Désignation Universelle(2)..... 9
4. L'organisation 10
Les Informations du DNS : Classe et type..... 11
Les composants..... 12
A l'intérieur d'une zone..... 13
Résolution des noms en adresses..... 14
La résolution "itérative"..... 15
La résolution"récursive" 15
Le format des requêtes 16
Les requêtes inverses..... 17
Un exemple de client : nslookup..... 18
5. L'administration..... 21
Conclusion 22
Bibliographie..... 23

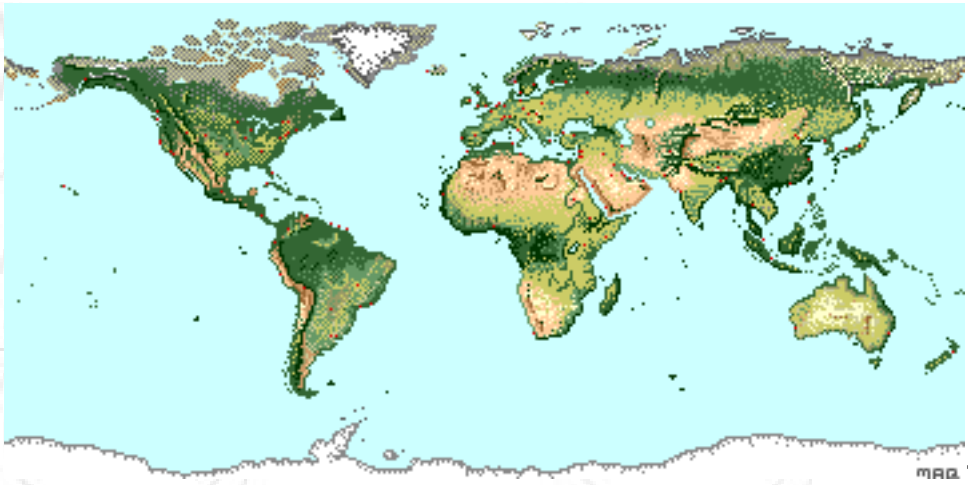
Laurence Duchien

1. L'Internet

L’Internet est le résultat de l’interconnexion de réseaux informatiques très variés, mais évidemment capables de communiquer.

L’Internet :

- Un système de liaisons physiques (réseaux locaux, réseaux de campus, réseaux régionaux, liaisons nationales et internationales),
- Un langage commun (TCP/IP)
- Des règles de fonctionnement (pas toujours explicites)
- Des applications : messagerie, transfert de fichiers, forum, systèmes d’informations, annuaires...
- Une administration centrale très légère... on joue la carte de la décentralisation.



Utilisation d’”autoroutes de l’information” : NSFnet aux USA, Renater en France.

Quelques Caractéristiques

· Le plus grand réseau informatique du monde (environ 5 millions de machines, 100 % de croissance annuelle, environ 30 millions d'utilisateurs).

Pour mémoire :

- 69 :DOD lance le réseau Arpanet

- 70-80 : définition de TCP/IP, mise en place de réseaux en France de même type (Transpac...)

- 80 : séparation Milnet-Arpanet, mise en place de NSFnet

- 90 : L'Internet s'ouvre au public (en 92 : plus de sites commerciaux qu'universitaires, en 94 : arrêt des subventions de la NSFnet)

· Une administration centrale très légère et très décentralisée (l' anarchie ?)

ISOC : (Internet Society) organe d'orientation générale, évaluation des technologies, président : CH Huitema (INRIA).

IAB : (Internet Architecture Board) responsable des standards

IETF (Internet Engineering Task Force) Organise des réunions ouvertes à tous

InterNIC (Internet Network Information Center) attribution des adresses, pages blanches, statistiques,...

· Fondé sur un effort coopératif et nécessite donc une volonté réciproque.

· L'explosion actuelle du réseau ne va pas sans poser des problèmes : techniques, organisationnels, financiers et sécuritaires.

· La règle essentielle : **confiance et coopération**; c'est à dire le respect du travail de chacun, c'est ce que l'on appelle l'Esprit Internet.

Type d'utilisation

- 53% usage commercial
- 27% recherche
- 9% administration
- 5% formation, éducation

Les organismes publics :

- Les centres de recherche (présentation, rapports techniques, logiciels,...)
- Les bibliothèques (catalogue en ligne, diffusion de fac-similés,...)
- Les administrations (organismes internationaux, ministères, régions collectivités locales, texte de loi,...)
- Les agences (statistiques, annonces de conférences, normes,...)

Les individus

- Services d'archives, envois de disquettes, création et diffusion de logiciels, envois dans les forums, création de rubriques personnelles sur des serveurs d'employeur, piratage...

Les entreprises

- gratuit : présentation générale de l'entreprise, vente par correspondance, documentation produits, manuels d'utilisation
- payant : journal électronique, banque de données

(pas de tarification à la connexion)

Les Moyens

Le réseau dans son ensemble fournit des moyens :

• pour accéder à une machine

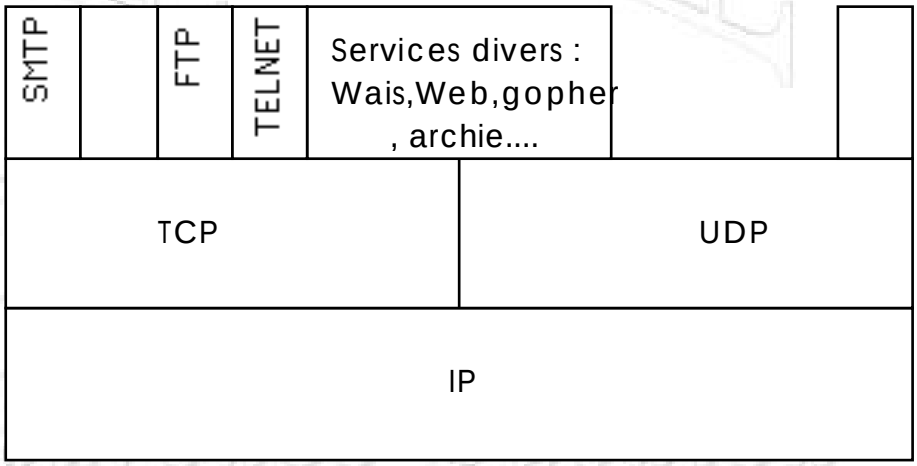
• pour partager des ressources informatiques

• pour communiquer entre personnes

• pour accéder à de l'information

Le modèle utilisé pour l'ensemble des applications :

architecture client- serveur



- terminal virtuel : telnet

- transfert de fichiers : ftp

- messagerie : mail et smtp

- les autres services : le serveur de noms DNS, Wais, Gopher, Web, archie,

- l'administration de réseaux : SNMP

2. Le problème de la résolution de noms en adresse

Dans un réseau, les machines ont un nom (logique) et une adresse (physique).

exemple :

ftp leguin.cnam.ft (nom)

ftp 192.33.159.6 (adresse)

Pour rendre la vie plus facile à l'utilisateur final, on utilise un système d'annuaire:

- Sert à stocker une ensemble d'informations utiles (surnoms, noms de responsables, adresse postale des sites,...)

- Correspond à une base de données distribuées dont il faut gérer les pb de performances et la cohérence des données)

Laurence Duchien

3. La Désignation Universelle

Un **nom symbolique** sert à désigner une machine, un service, une adresse, une route pour les atteindre.

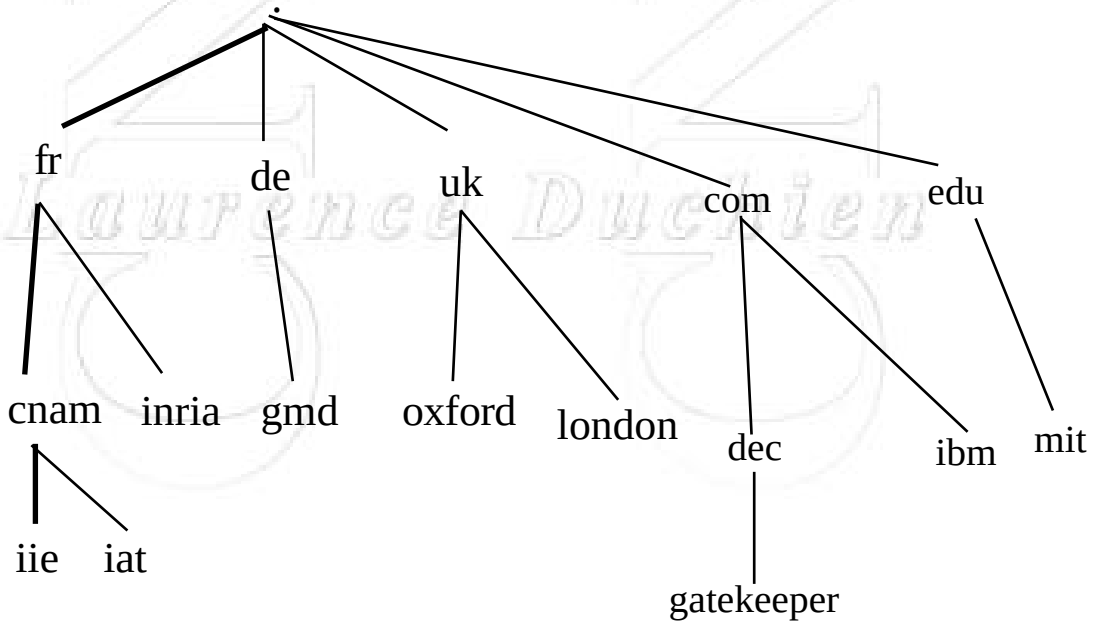
Le NIC (Centre d'information du réseau Internet) gère le domaine des noms et détermine si les noms proposés sont acceptables.

Le système des domaines est un système hiérarchique. Ce qui permet de ne pas avoir à faire à une administration centrale à chaque fois que l'on rajoute une machine dans son réseau local.

Désignation : objet.sous-domaine.domaine

Objet : nom d'une machine, par exemple (rubis) ou de service (ftp.cnam.fr)

Domaine : politiques (fr, de, jp, nl,...) ou institutionnels (com, mil, gov, edu, net,...)



On écrit un nom en séparant les noeuds par des points, la racine étant à droite. ex : iie.cnam.fr

3. La Désignation Universelle(2)

- Les noeuds terminaux de l'arborescence du DNS sont des machines.

- Un domaine est un nom non terminal de l'arborescence.

- Du fait de l'arborescence, un nom simple (iie par exemple) n'a aucune raison d'être unique, seuls les noms développés sont uniques (iie.cnam.fr).

-> Cela permet aux administrateurs d'ajouter des machines sans prévenir les autorités centrales.

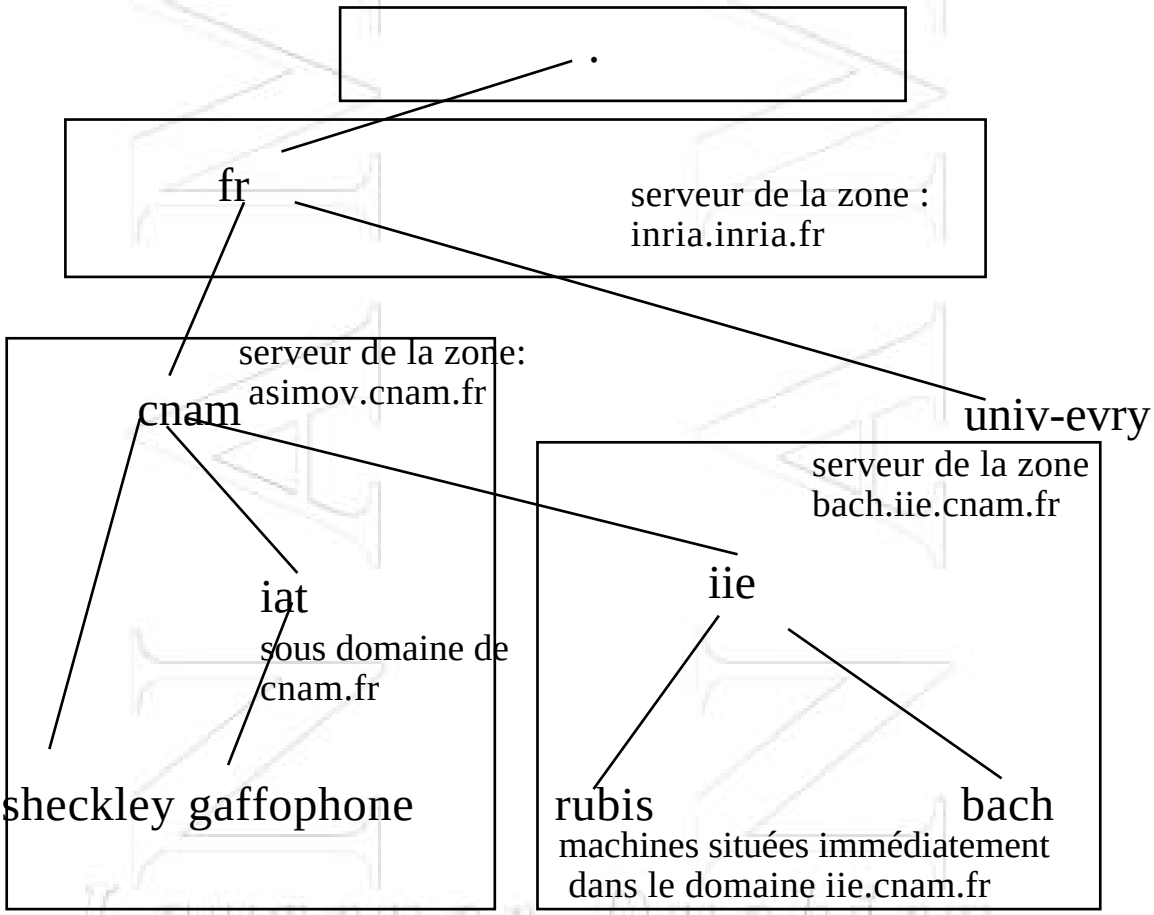
- Il faut aussi noter que la hiérarchie du DNS n'a pas grand chose à voir avec la topologie physique de l'Internet qui est un graphe.

- La profondeur de l'arbre est variable : les feuilles se trouvent en général au 3 eme ou 4 eme niveau.

Laurence Duchien

4. L'organisation

- On parle de **Zone** pour une partie contiguë de l'arborescence sur laquelle un serveur a autorité.



Le DNS est partitionné.

Chaque zone a un ensemble de serveurs faisant autorité.

Les informations sont dupliquées physiquement sur ces serveurs

Aucun serveur DNS n'a une vue d'ensemble de l'Internet.

Les Informations du DNS : Classe et type

- le DNS stocke des informations pour des protocoles différents.
- Toute information stockée a une **classe** et un **type**.
- Les RR (“ressource records”) sont les enregistrements de la base
- La classe identifie le protocole par exemple.
- Le type identifie le type de donnée (adresse de machine A record, le serveur de noms d’un domaine NS record, un relais de courrier électronique MX record,...)
- L’enregistrement contient également la durée de vie, le TTL qui indique la période de validité
- L’enregistrement contient alors les données (RDATA)

  RR = {classe, type, clé, valeur}

- Exemple :

  {IN, A, munnari.oz.au, 128.250.1.21}

  IN : famille des protocoles de l'Internet

  A : Adresse

  cet enregistrement indique que la machine munnari.oz.au a pour adresse 128.250.1.21

- Autres exemples :

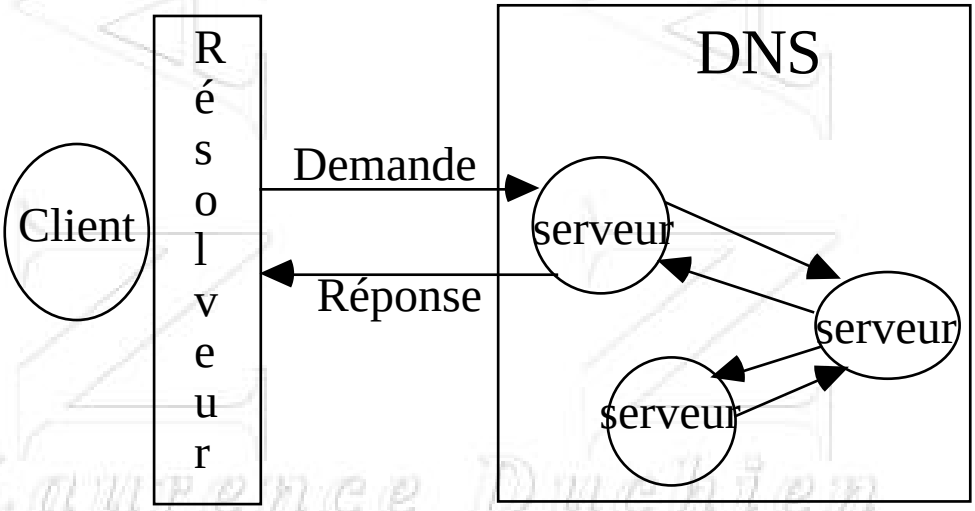
  {IN, MX, asimov.cnam.fr, chenas.inria.fr}

  {IN, HINFO, adso.melk.de, MONK}

  {IN, NS, cnam.fr, leguin.cnam.fr}

Les composants

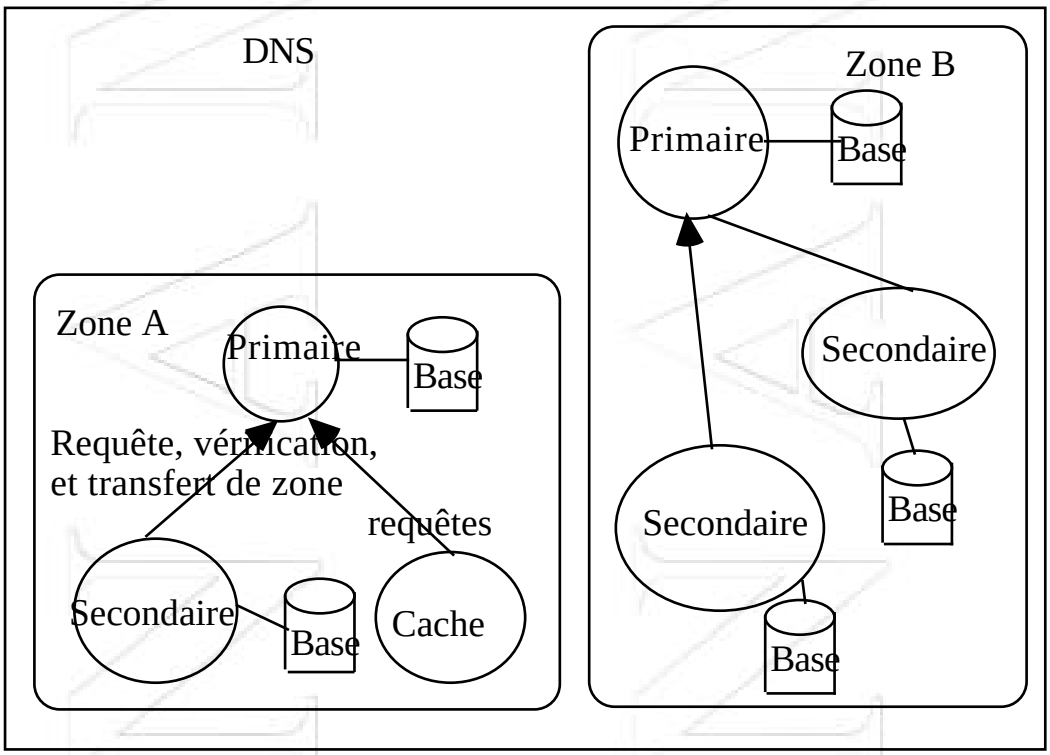
- Le processus de résolution est basé sur le modèle client-serveur.
- Un ou plusieurs serveurs possèdent des informations.
- Un client cherche ses infos et interroge un ou plusieurs serveurs, eux-mêmes pouvant demander des informations aux autres serveurs.
- L'agent du client s'appelle résolveur (sous-pgme d'une bibliothèque que l'on peut lier avec un pgme).Il est appelé par des routines Unix comme gethostbyname.



- Implantation de référence : BIND (Berkeley Internet Name Domain)

A l'intérieur d'une zone

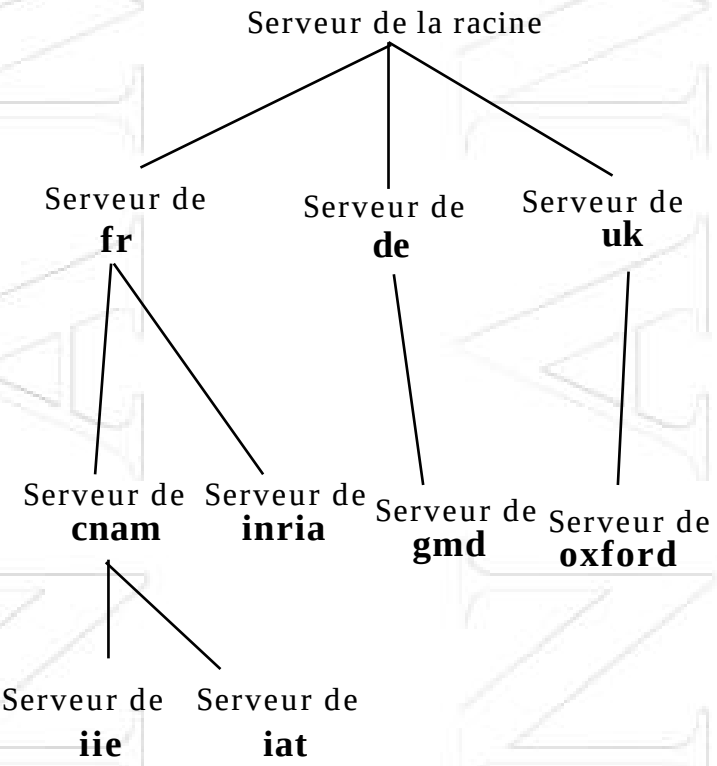
- Zone = 1 seule autorité administrative
- Un serveur primaire
- Plusieurs serveurs secondaires
- Des caches



Laurence Duchien

Résolution des noms en adresses

• Mise en correspondance des noms avec des adresses par l'utilisation de serveurs de noms distribués.



Laurence Duchien

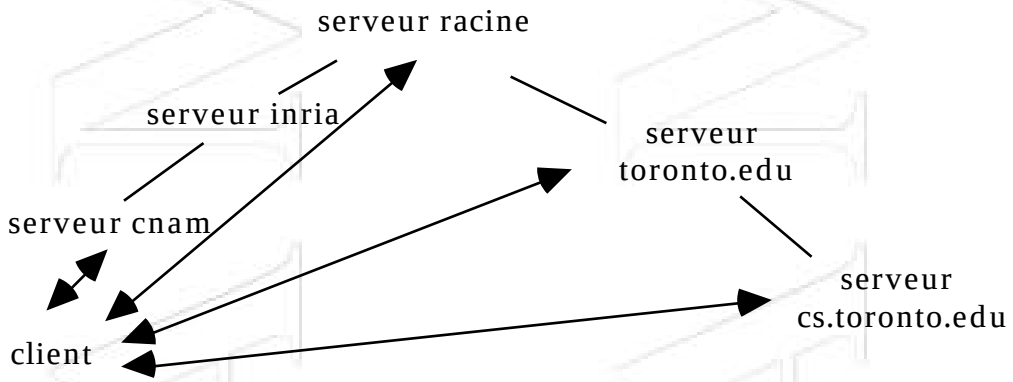
- Lorsqu'un serveur de noms reçoit une requête, il vérifie si le nom appartient à un sous-domaine dont il assure la gestion.

- si c'est le cas, il traduit le nom en adresse et joint la réponse à la demande avant de renvoyer le tout au client.

- si ce n'est pas le cas, il vérifie le type d'interaction demandée par le client (récursive ou interactive)

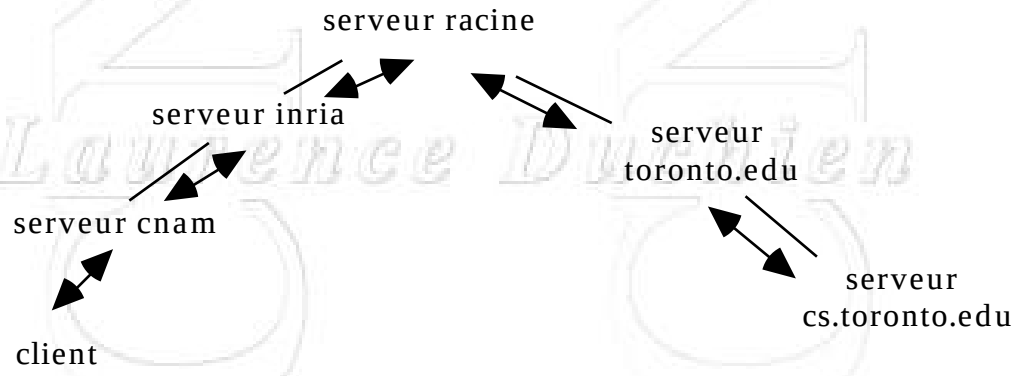
La résolution "itérative"

Le client interroge chaque serveur successivement qui lui indique quel est le successeur à interroger pour obtenir la traduction.



La résolution"récursive"

Chaque serveur résout à son niveau le reste du nom.



- Pour plus d'efficacité, on utilise des caches.
- Les noms récemment utilisés sont enregistrés dans une mémoire cache.
- Lorsqu'un client demande un nom, le serveur vérifie que celui-ci n'est pas dans la mémoire cache.

Le format des requêtes

- Les requêtes ont un type : QTYPE (query type)
- Les deux formes de type sont RR (A, CNAME, MX, etc,...) ou * (any)

exemple RR :

{IN, A, munnari.oz.au, ?} =>

{IN, A, munnari.oz.au, 128.25.1.21}

{IN, MX, cnam.fr, ?} =>

{IN, MX, cnam.fr, chenas.inria.fr}

{IN, A, chenas.inria.fr, 128.93.8.8}

Exemple *:

{IN,* , toaster.scott.aq, ?} =>

{IN,A , toaster.scott.aq, 192.133.31.4}

{IN,HINFO , toaster.scott.aq, {IBM-toaster, MVS}}

{IN,MX , toaster.scott.aq, {nowhere.lost.aq,10}}

{IN,A , nowhere.lost.aq, 192.133.31.5}

- Les requêtes sont portées dans des paquets UDP.
- Les requêtes de mises à jour sont faites par les administrateurs en modifiant les bases.

Les requêtes inverses

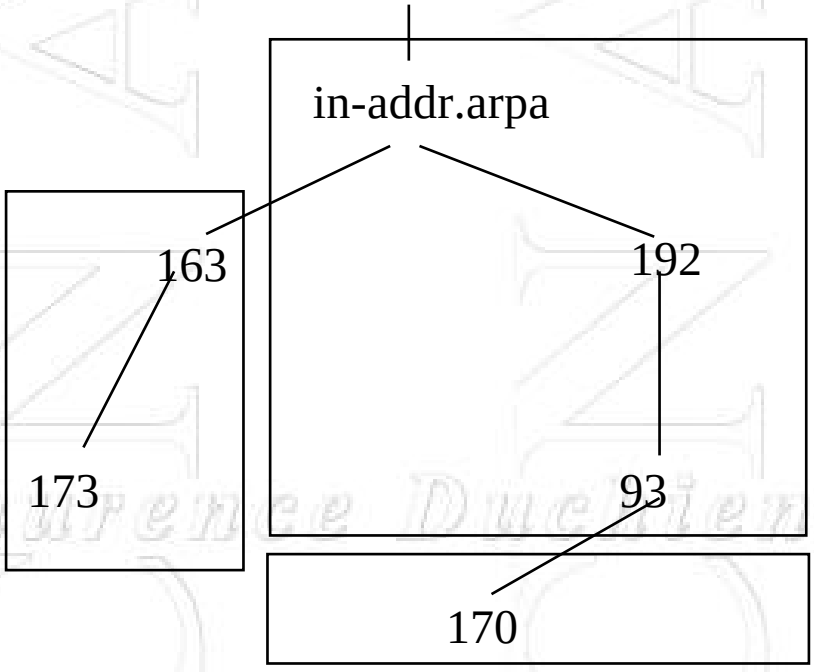
- Les requêtes inverses (requête à partir d'une valeur et non d'une clé) sont aussi possibles.
- traduire une adresse IP en nom =>

les serveurs ftp demandent un nom lors d'une connexion pour enregistrer la transaction.

Le serveur n'a qu'une information l'adresse IP du client

IP ne connait pas le DNS

=> On utilise un domaine spécial **inaddr.arpa** qui a la structure suivante :



- Les requêtes sont de type PTR ("pointeur").
- Pour la recherche du nom de la machine dont l'adresse est 192.133.31.4 :

{IN, PTR, 4.31.133.192.in-addr.arpa, ?}

=> {IN, PTR, 4.31.133.192.in-addr.arpa, toaster.scott.aq}

Un exemple de client : nslookup

- Unix Berkeley
- destiné au déboguage des serveurs

```
% nslookup
Default Server:  asimov.cnam.fr
Address:  163.173.128.6
> athena.mit.edu
Server:  asimov.cnam.fr
Address:  163.173.128.6

Name:    athena.mit.edu
Address:  18.72.0.39

> sheckley.cnam.fr
Server:  asimov.cnam.fr
Address:  163.173.128.6

Name:    sheckley.cnam.fr
Address:  163.173.128.192

> asimov.cnam.fr
Server:  asimov.cnam.fr
Address:  163.173.128.6

Name:    asimov.cnam.fr
Address:  163.173.128.6

> set type=MX
> inrets.fr
Server:  asimov.cnam.fr
Address:  163.173.128.6

Non-authoritative answer:
inrets.fr       preference = 10, mail exchanger = orion.inrets.fr
Authoritative answers can be found from:
orion.inrets.fr inet address = 137.121.1.1
deneb.inrets.fr inet address = 137.121.1.2
layon.inria.fr  inet address = 192.93.0.4
```

```
> kuis.kyoto-u.ac.jp
Server:  asimov.cnam.fr
Address:  163.173.128.6

kuis.kyoto-u.ac.jp      nameserver = ns.kuins.kyoto-u.ac.jp
kuis.kyoto-u.ac.jp      nameserver = kudpc.kudpc.kyoto-u.ac.jp
kuis.kyoto-u.ac.jp      nameserver = isfs.kuis.kyoto-u.ac.jp
kuis.kyoto-u.ac.jp      nameserver = kuis.kuis.kyoto-u.ac.jp
kuis.kyoto-u.ac.jp      origin = isfs.kuis.kyoto-u.ac.jp
        mail addr = ns-admin.kuis.kyoto-u.ac.jp
        serial=20312, refresh=3603, retry=300, expire=3600000, min=3600
kuis.kyoto-u.ac.jp      inet address = 130.54.23.3
kuis.kyoto-u.ac.jp      preference = 50, mail exchanger = isfs.kuis.kyoto-u.ac.jp
kuis.kyoto-u.ac.jp      preference = 100, mail exchanger = hemp.imel.kyoto-u.ac.jp
ns.kuins.kyoto-u.ac.jp  inet address = 130.54.8.22
ns.kuins.kyoto-u.ac.jp  inet address = 130.54.254.1
kudpc.kudpc.kyoto-u.ac.jp       inet address = 130.54.8.13
kudpc.kudpc.kyoto-u.ac.jp       inet address = 130.54.9.242
isfs.kuis.kyoto-u.ac.jp inet address = 130.54.23.2
kuis.kuis.kyoto-u.ac.jp inet address = 130.54.23.3
hemp.imel.kyoto-u.ac.jp inet address = 130.54.23.41
> ls -d services.sf.cnam.fr > voir
> view voir
 services-53             CNAME ntalk/udp.services.sf.cnam.fr
 33147                   CNAME ptpct147/udp.services.sf.cnam.fr
 services-54             CNAME efs/tcp.services.sf.cnam.fr
 33150                   CNAME ptpct150/udp.services.sf.cnam.fr
 33148                   CNAME ptpct148/udp.services.sf.cnam.fr
 34170/udp               CNAME tpbgi170/udp.services.sf.cnam.fr
 services-55             CNAME route/udp.services.sf.cnam.fr
 33149                   CNAME ptpct149/udp.services.sf.cnam.fr
 services-56             CNAME timed/udp.services.sf.cnam.fr
 services-57             CNAME tempo/tcp.services.sf.cnam.fr
 20113/tcp               CNAME mvtcp13/tcp.services.sf.cnam.fr
 services-60             CNAME netnews/tcp.services.sf.cnam.fr
 services-58             CNAME courier/tcp.services.sf.cnam.fr
 netstat/tcp             TXT  netstat:15:tcp
 services-61             CNAME netwall/udp.services.sf.cnam.fr
 services-59             CNAME conference/tcp.services.sf.cnam.fr
 tpbgi140                TXT  tpbgi140:34140:
 34190/tcp               CNAME tpbgi190/tcp.services.sf.cnam.fr
 34210/tcp               CNAME tpbgi210/tcp.services.sf.cnam.fr
 services-62             CNAME uucp/tcp.services.sf.cnam.fr
 printer/tcp             TXT  printer:515:tcp:spooler
```

5. L'administration

- S'enregistrer auprès de domaine du dessus (fr)
- Sous-diviser son domaine
- déclarer 1 serveur primaire, des serveurs secondaires, des caches
- Créer des bases permanentes

Les enregistrements (SOA : Start Of Authorithy) de la base permanente contiennent des infos sur les caractéristiques de la zone (serveur maître, adresse de l'administrateur, no de série des informations actuelles, critères de mises à jour...)

Exemple :

```
; les infos sur l'autorité
@ INSOA        cnam.fr      root.cnam.cnam.fr (
                            92120712        ; serial
                            300             ; Refresh -5 mn
                            60              ; retry -1 mn
                            1209600         ; Expire - 2 weeks
                            43200)          ; minimum- 12 hours
; Les serveurs de la zone
    INNS       asimov.cnam.fr
    INNS       Sheckley.cnam.fr
    INNS       Layon.inria.fr
; Les machines
farmer         IN    A      163.173.128.1
cisco          IN    A      163.173.128.2
asimov         IN    A      163.173.128.6
               IN    MX     10    chenas.inria.fr
ftp       IN   CNAME        asimov
bindmaster     IN    CNAME        asimov....
```

Conclusion

Très souple,

Permet des extensions - comme Hesiod (serveur des utilisateurs et des services)

- comme l'ajout de type supplémentaires dans la classe IN

efficace, robuste, indispensable,...

Avec quelques extensions => concurrent très sérieux de X500

Laurence Duchien

Bibliographie

. TCP/IP Architecture, protocoles, applications, Comer, Intereditions

. DNS and BIND, Nutshell, O'Reuilly

. Les articles S.Bortzmeyer accessibles par ftp.cnam.fr, /pub/...

. Les news

. Le poly de TP "Internet" de la valeur Réseaux et communications, L.Duchien, E. Gressier, CNAM , 95.

Laurence Duchien