DNS

DNS – Domain Name Service

Il est difficile de mémoriser les adresses IP dans le cas d'un grand réseau

On peut **désigner** les ordinateurs d'un réseau par **des noms logiques** faciles à mémoriser il faut donc pouvoir faire l'association entre ceux-ci et l'adresse IP

Cette association peut se faire:

1. Par une table située dans le **fichier hosts** de chaque machine
2. Par une table gérée par un **serveur de DNS**, chaque machine connaissant l'adresse de ce dernier

Sur Internet c'est le fournisseur d'accès qui rempli ce rôle

Qu'est le DNS

Base de donnée (Client Serveur) en ligne permettant de **transformer les noms de domaine complets FQDN** (Full Qualified Domain Name) en **adresse IP**

Si vous êtes connecté à un fournisseur d'accès internet (FAI) de façon intermittente par PPP, ADSL ou autres, ce sont généralement **les serveurs DNS de votre FAI** qui assurent la résolution des noms,

DNS France Telecom (wanadoo):
@193.252.19.3 ou 4

Le DNS fonctionne au **niveau de la couche application** et utilise les protocoles UDP et parfois TCP de la couche transport

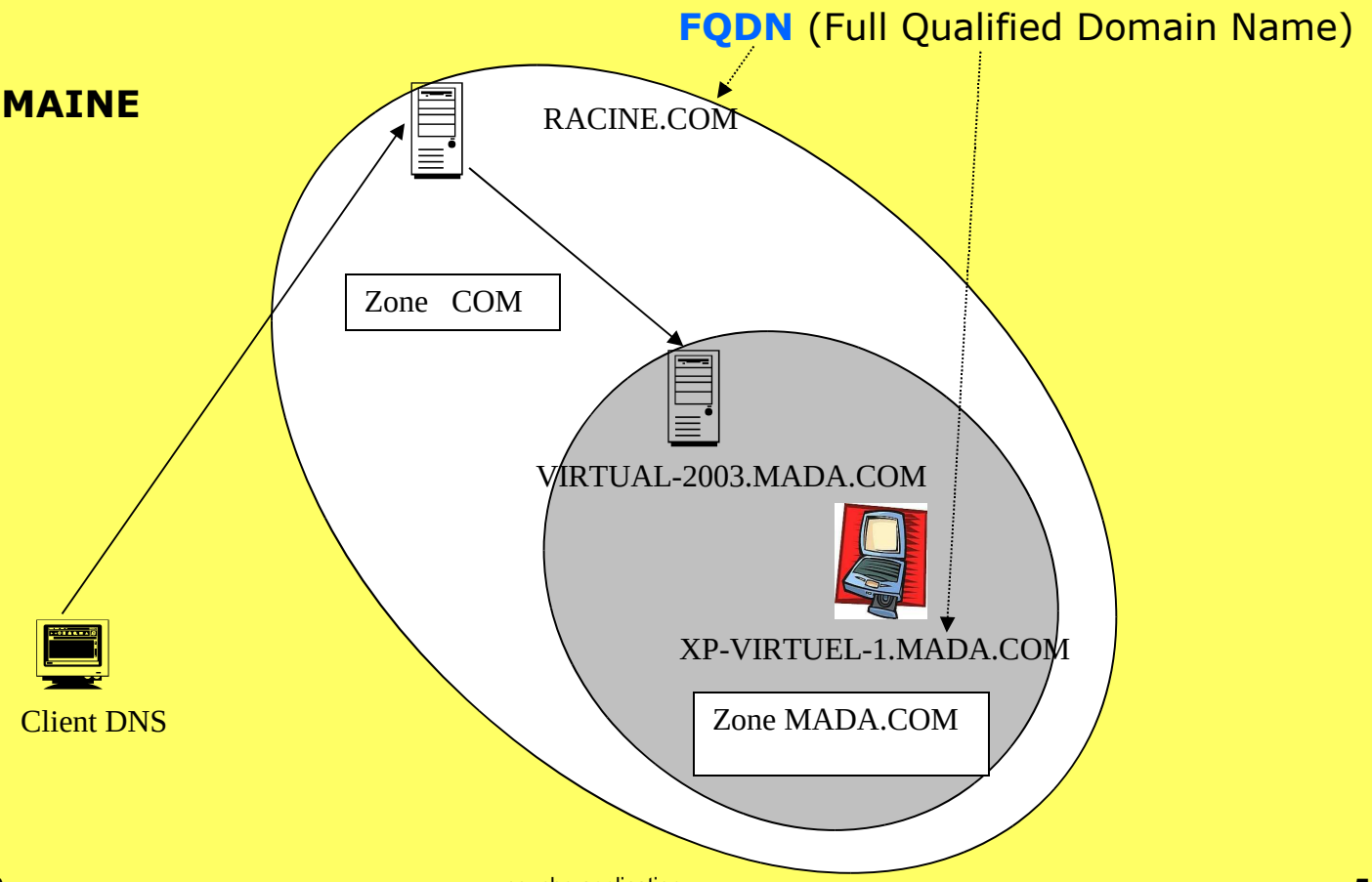
Clients = resolvers
Serveurs = name servers

Nom de domaine

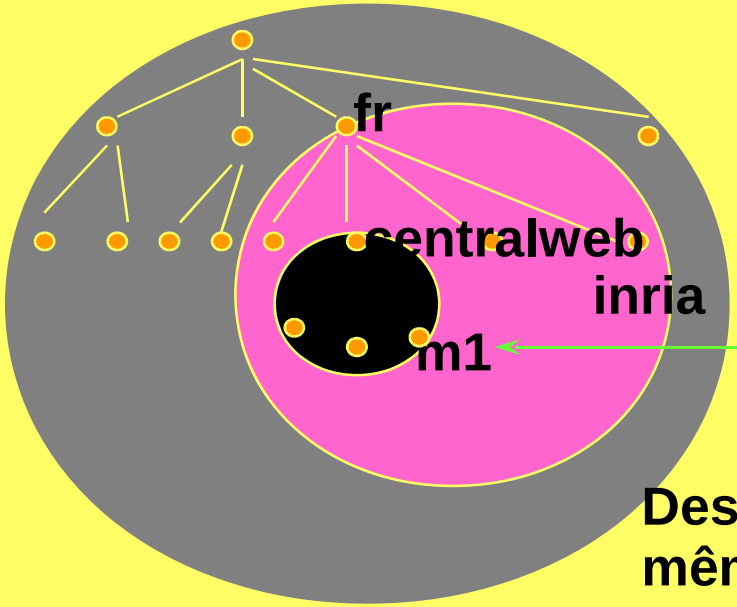
- Un nom de domaine est un index dans la base DNS; exemple :
  - m1.centralweb.fr pointe vers une adresse IP
  - centralweb.fr pointe vers des informations de
  - fr pointe vers des informations

Le domaine dans un LAN

ZONE = DOMAINE



Le domaine dans un WAN



- Domaine complet
- Domaine fr
- Domaine centralweb

noeud m1.centralweb.fr

Des noeuds peuvent avoir les mêmes noms dans des domaines différents : ns.centralweb.fr et ns.renault.fr

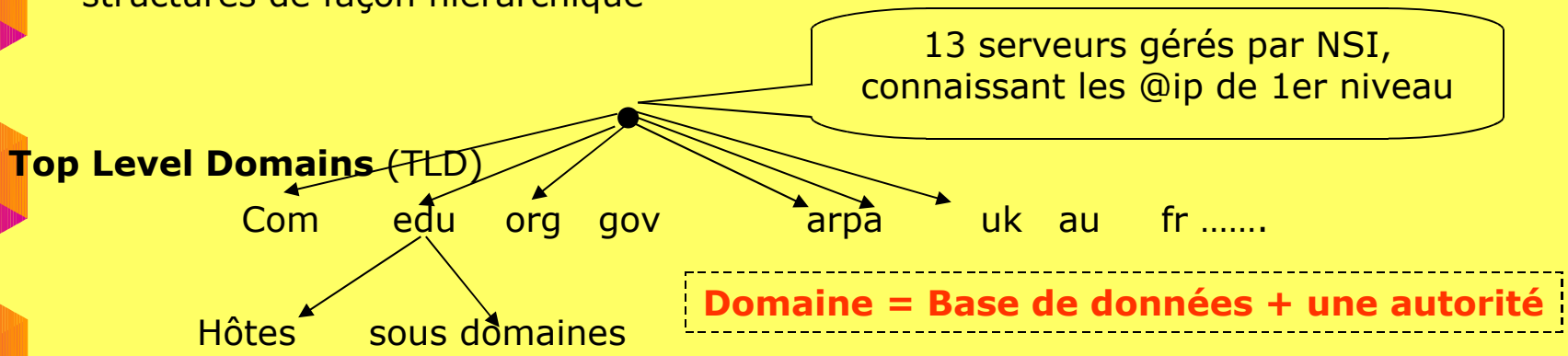
Le système est mis en œuvre par une base de données distribuée au niveau mondial

Les noms sont gérés par un organisme mondial : l'interNIC et les organismes délégués : RIPE, NIC France, NIC Angleterre, etc.

- **Chaque noeud est identifié par un nom**
- **Racine appelée root, identifiée par «.»**
- **127 niveaux au maximum**

DNS organisation arborescente (wan)

Les serveurs sont regroupés dans des domaines (rien à voir avec les domaines NT) structurés de façon hiérarchique



Domaine = Base de données + une autorité

Hôte. sous dom.sous dom.domaine = Full Qualified Domain Name

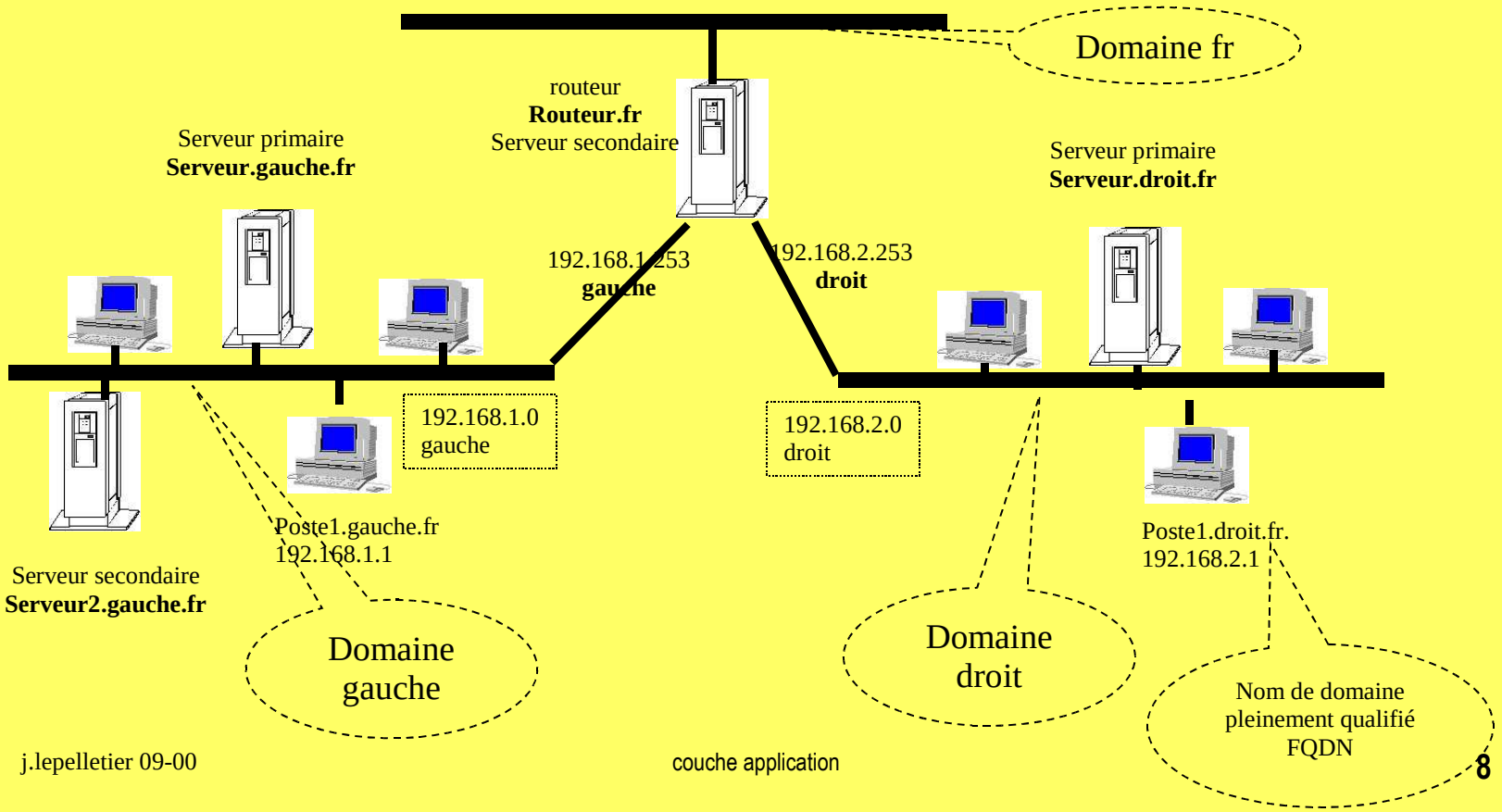
www.Microsoft .com

Il faut lire ces noms de domaines de droite à gauche en partant donc du plus général vers le plus particulier.

Deux noeuds fils ne peuvent avoir le même nom ==> unicité d'un nom de domaine au niveau mondial

DNS organisation arborescente (local)

Un réseau important doit-être divisé en domaines ou zones possédant chacun un serveur DNS



13 serveurs clés

Identifiés par une lettre de l'alphabet

Fichier des adresses => ftp://ftp.rs.internic.net/domain/named.root

Domaines racine

- Le système DNS impose peu de règles de nommage :
  - noms < 63 caractères
  - majucules et minuscules non significatives
  - pas de signification imposée pour les labels
- Le premier niveau de l'espace DNS fait exception à la règle :
  - 7 domaines racines prédéfinis :
    - com : organisations commerciales ; ibm.com
    - edu : organisations concernant l'education ; mit.edu
    - gov : organisations gouvernementales ; nsf.gov
    - mil : organisations militaires ; army.mil
    - net : organisations réseau Internet ; worldnet.net
    - org : organisations non commerciales ; eff.org
    - int : organisations internationales ; nato.int
  - arpa : domaine reservé à la résolution de nom inversée
  - organisations nationales : fr, uk, de, it, us, au, ca, se, etc.

Serveur de nom

Serveur de nom = processus répondant aux requêtes DNS

Serveur de nom = Machine + Base de données en ASCII + logiciel de recherche

Le logiciel le plus courant est BIND (Berkeley Internet Name Domain)

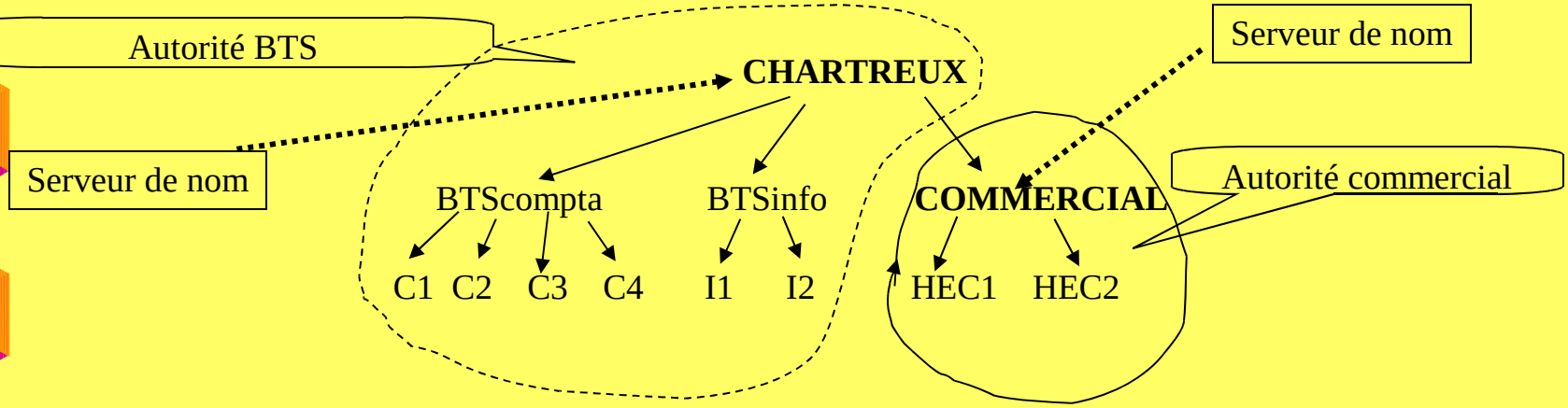
Un domaine peut avoir plusieurs serveurs de noms
un primaire → original de la base
un ou des secondaires copies de la base

Un nom d'hôte correspond à une @ip
Une machine peut avoir plusieurs @ ip

Zone d'autorité

Un serveur de noms ne s'occupe pas d'un seul nœud de l'arborescence, mais d'un **ensemble de nœuds** sur lequel il aura autorité. (Authoritative Name Server).

Une zone d'autorité recouvre au moins un domaine, appelé domaine racine de la zone et peut inclure des sous-domaines mais pas forcément tous les sous-domaines .



Un nœud de réseau est une machine qui peut être adressée

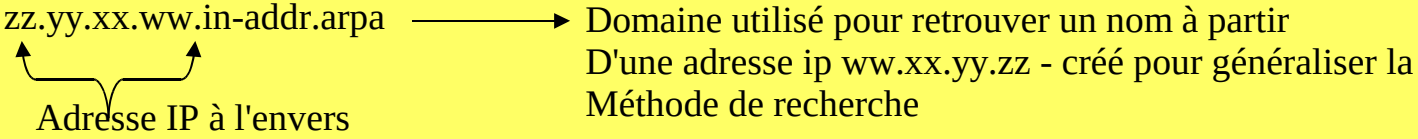
Domaine inverse

Le principe de la résolution de nom, consiste à affecter un nom à une adresse IP.
Le processus inverse doit pouvoir également être mis en œuvre.
Pour cela il y a un domaine particulier, in-addr.arpa, qui permet la résolution inverse d'adresse IP qui permet, à partir d'une adresse IP, de trouver son nom d'hôte.

Pour le réseau 192.168.1.0, on créera une zone inverse dans le domaine in-addr.arpa. La zone de recherche inverse dans le domaine deviendra:

1.168.192.in-addr.arpa

On inscrira dans cette zone tous les nœuds du réseau pour lesquels on désire que la résolution inverse fonctionne.



Cache DNS

Chaque enregistrement contient une durée de validité des informations. Une fois qu'une machine cliente a obtenu une information, l'enregistrement est valide pour le temps donné.

Après cette durée, il faut a nouveau demander cette information.

Pendant cette durée, l'information est stockée dans un *cache*.

La présence de ce mécanisme de cache dans tous les serveurs de noms ainsi que dans un certain nombre de clients permet de limiter le nombre de requêtes faites, au prix d'une certaine latence dans la mise à jour d'informations quand un changement est fait.

Commandes agissant sur le cache

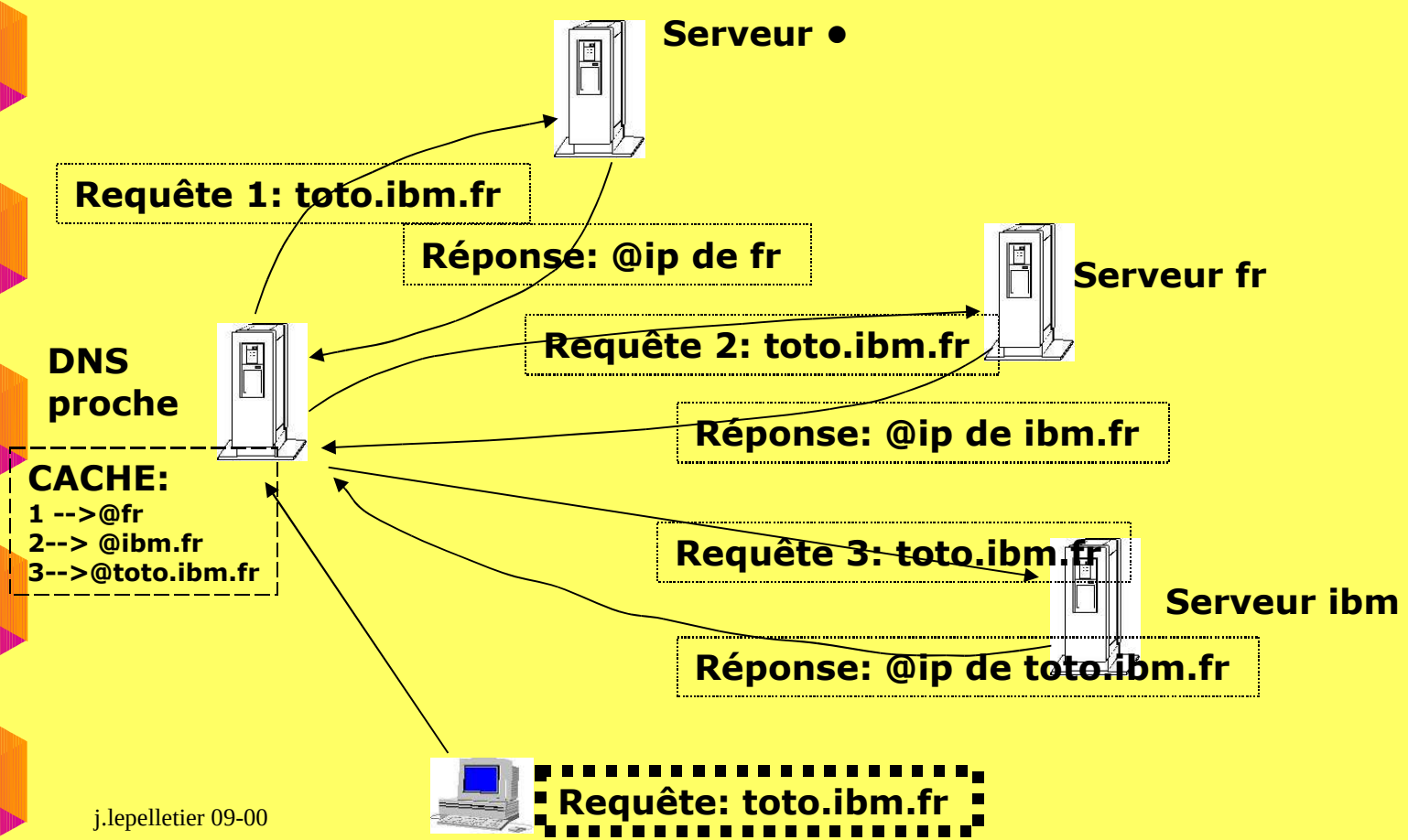
ipconfig /flushdns]

Vide le cache du client DNS

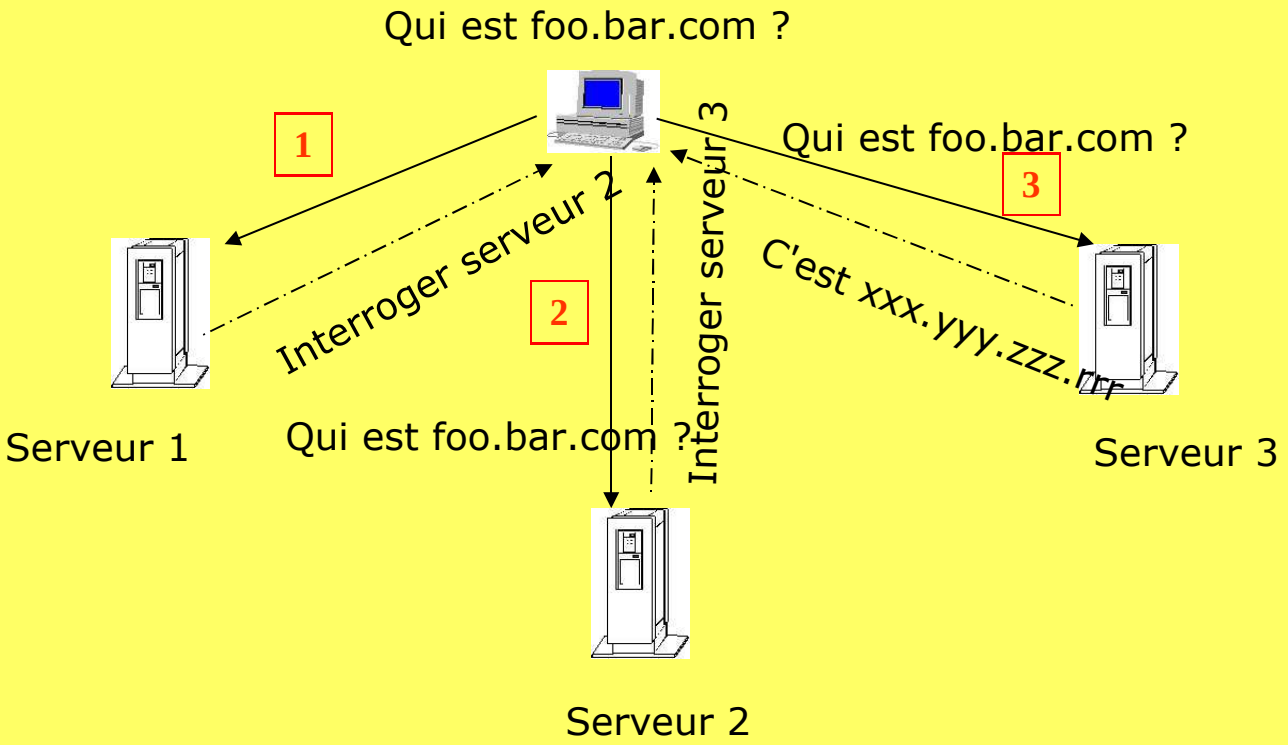
Ipconfig /displaydns

Visualise le cache DNS

Stratégie de requête récursive



Stratégie de requête itérative



Configuration d'une machine cliente

Pour configurer une machine utilisant le service de noms, il faut toujours obtenir les informations suivantes:

- **Le nom de domaine** qui sera ajouté aux domaines non qualifiés.
- **La liste des serveurs** de noms qui seront interrogés par cette machine.

Le nom de domaine est *toujours* celui de votre organisation. C'est par exemple: chartreux.fr si vous êtes aux chartreux.

Si votre machine est serveur de noms (c'est à dire que votre machine exécute un processus serveur de noms, généralement appelé named sur une machine LINUX), vous devez indiquer votre propre machine comme serveur de noms. L'adresse IP à utiliser est *obligatoirement* 127.0.0.1 (localhost), il ne faut pas utiliser l'adresse 0.0.0.0).
Si votre machine n'est pas serveur de noms (cas de tous les ordinateurs personnels), vous devez demander à votre administrateur réseau quels sont les machines serveurs de noms dans votre organisation. (stocké dans /etc/resolv.conf sous linux)

Base de données DNS

La base de données DNS est constituée d'enregistrements appelés RR (ressource record)

Chaque RR est constitué de:

Domaine --> nom du domaine concerné
ttl --> time to leave temps en seconde pendant lequel l'information peut rester en cache
classe -->IN pour les @ip
type --> type de l'enregistrement RR
données --> info associées au type

SOA --> concernant le domaine
Origine --> nom du domaine
Contact --> adresse du responsable
Série --> numéro de version du SOA
rafraîchissement --> temps de rafraîchissement du serveur secondaire
….

Base de données DNS

NS --> spécifie le serveur primaire et les secondaires

A --> associe nom d'hôte et @ip

CNAME --> associe un alias à un hôte

PTR --> pointeur utilisé pour la recherche inverse

Etc…

DNS sous linux

Le fichier /etc/resolv.conf

Avant de configurer le DNS (Domain Name System - Système des noms de domaines), il faut vérifier le contenu du fichier :

/etc/resolv.conf.

Il doit contenir un champ domain suivi du nom de votre domaine (ar exemple nunux.fr).
Il doit aussi contenir une ligne commençant par nameserver suivi de l'adresse IP du serveur DNS.
Si ce dernier est un PC personnel, alors l'adresse sera 127.0.0.1.

Voici un exemple de fichier /etc/resolv.conf:

```
domain nunux.fr
nameserver 127.0.0.1
```

Vous devez aussi installer le package bind qui contient le programme named qui est le serveur de nom.

DNS sous linux

Création du fichier /etc/named.conf
Ce fichier (quelques octets) ne contient que des pointeurs vers les fichiers de référence.
exemple de fichier /etc/named.conf :

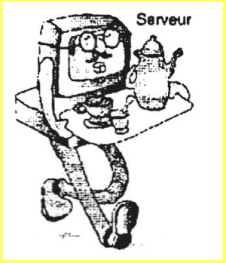
```
zone "0.0.127.in-addr.arpa" {
   type master;
   file "/var/named/pz/127.0.0";
};
zone "0.168.192.in-addr.arpa" {
   type master;
   file "/var/named/pz/192168.0";
};
zone "nunux.fr" {
   type master;
   file "/var/named/pz/nunux.fr";
};
```

La première partie sert à la résolution inversée des noms. Cela permet de connaître le nom d'un PC à partir de son adresse IP
Par utilisation d'un nom de domaine particulier:
in-addr.arpa

La deuxième partie sert à la résolution de noms du domaine nunux.fr

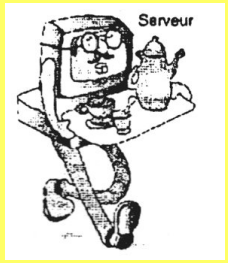
..

Types de serveurs de noms



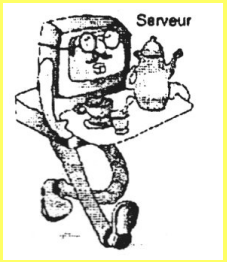
principal

Connaît l'original de la base de données de définition d'une zone



secondaire

Détient une copie d'une base de données



cache

Contient les réponses aux requêtes précédentes et interroge les serveurs primaires et secondaires

Une zone est un ensemble ou une portion de domaine

Un **serveur PRINCIPAL** est un serveur qui **gère un fichier de zone** en lecture/écriture. C'est généralement **le SOA**.
Il **peut dupliquer** sa base de compte vers d'autres machines, un serveur principal DNS peut recopier tout ou partie de ses fichires de zone vers d'autres serveurs DNS (la base recopiée est en lecture seule).

On appelle **SERVEUR MAÎTRE** un serveur qui exporte un fichier de zone, et SERVEUR SECONDAIRE un serveur DNS qui reçoit un fichier de zone…
Un serveur maître peut être un Principal qui exporte les zones qu'il gère, mais aussi un secondaire exportant vers un autre serveur des zones qu'il a lui-même importées

On appelle **SECONDAIRE** tout serveur DNS qui importe un fichier de zone, c'est à dire qui peut résoudre des noms depuis un fichier qu'il ne gère pas, mais importe depuis un autre serveur.

Un serveur DNS **REDIRECTEUR** est un serveur DNS qui concentre les résolutions de noms des clients d'un réseau et est chargé de les transmettre à d'autres serveurs DNS compétents pour résoudre (SOA ou secondaires). Il fait office de concentrateur

un **SERVEUR DE CACHE** uniquement ne gère aucun fichier de zone et n'en importe aucun. Il n'est ni principal, ni secondaire.
Les seuls mappages qu'il connaît sont **ceux qu'il a résolu** (par des requètes itératives) suite à des demandes (récursives) de la part de résolveurs.
Un serveur de ce type est utile pour **décharger** les serveurs DNS de requètes souvent répétées car les adresses les plus demandées sont disponibles immédiatement, puisqu'elles sont en cache.

Outils d'administration

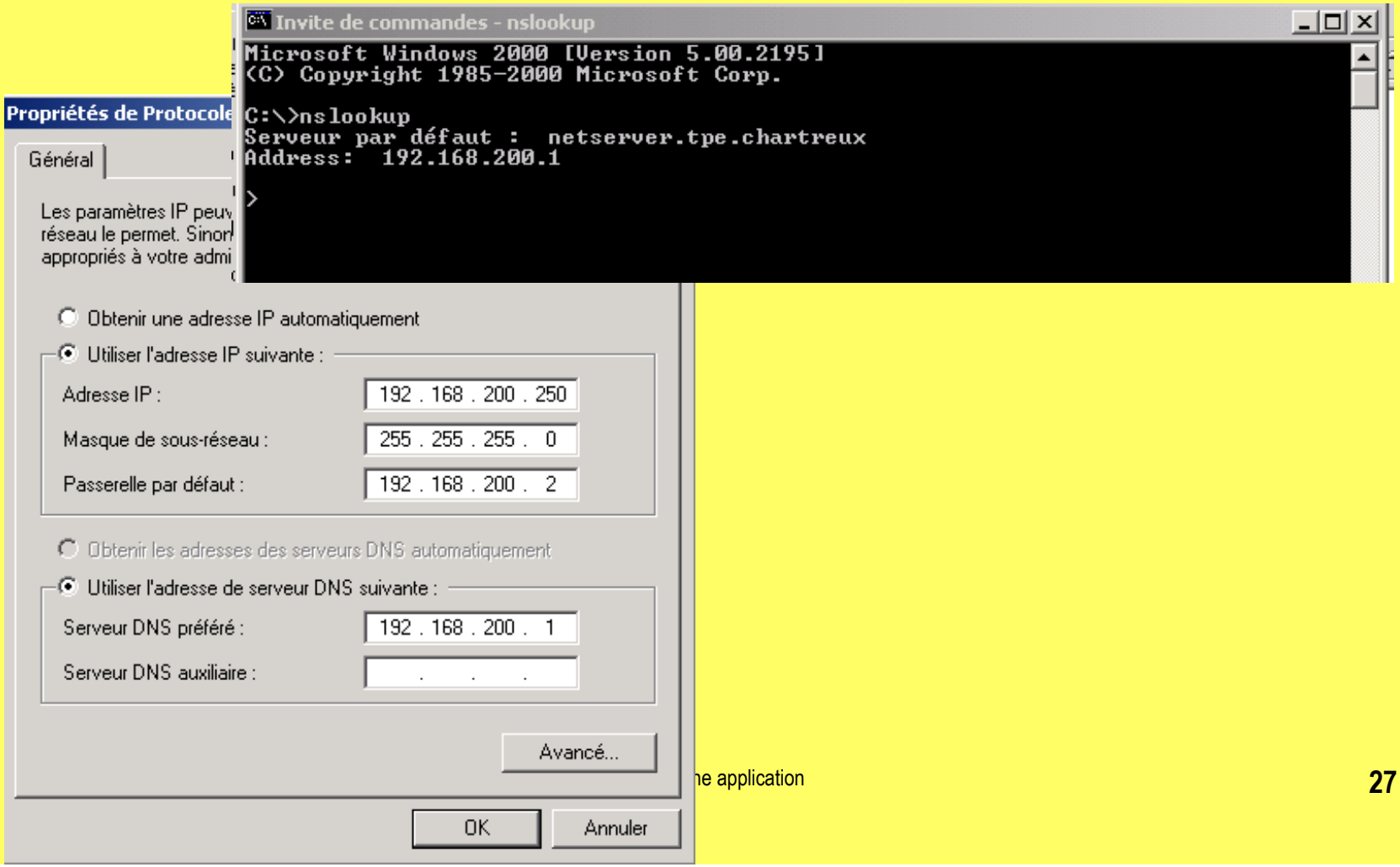
Nslookup Cet outil de diagnostic affiche des informations sur les serveurs de noms DNS (système de noms de domaine). **Nslookup** est disponible uniquement si le protocole TCP/IP est installé.

Nslookup

>set domain=resorts.ltree.com ← je cherche une station du domaine resorts.ltree.com
>instructor ← la station que je recherche est instructor
Server: unix.resorts.ltree.com ← le serveur que j'interroge
Address 144.19.75.15
Name : instructor.resorts.ltree.com la réponse
Address : 144.19.74.16

```
C:\>nslookup tpe.chartreux
Serveur :  netserver.tpe.chartreux
Address:  192.168.200.1

Nom :    tpe.chartreux
Served by:
- netserver.tpe.chartreux
          192.168.200.1
          tpe.chartreux
```

Exemple de nslookup



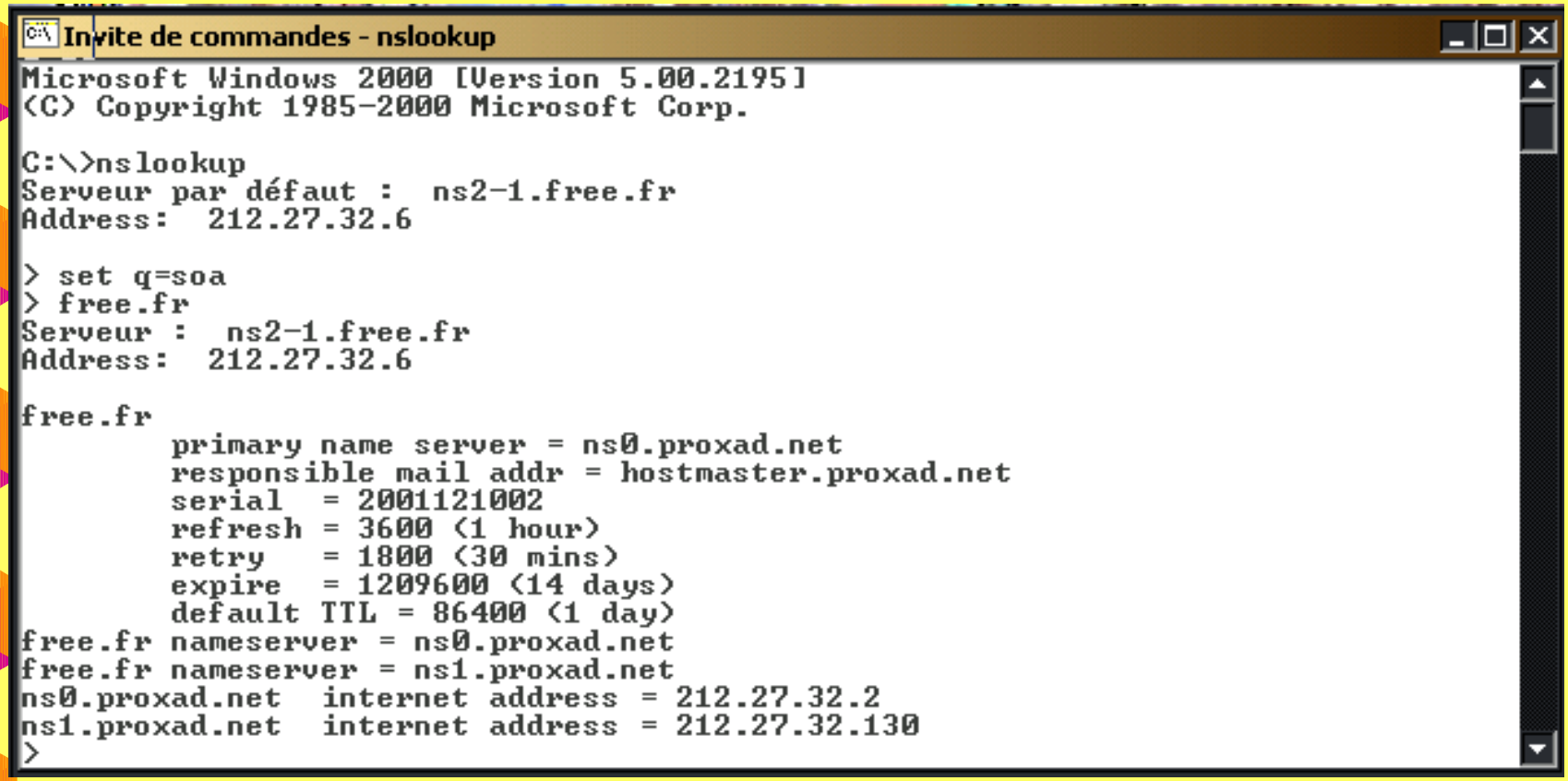
Exemple de nslookup

```
C:\>nslookup
Serveur par défaut :  netserver.tpe.chartreux
Address:  192.168.200.1
```

```
C:\>nslookup firewall.tpe.chartreux
Serveur :  netserver.tpe.chartreux
Address:  192.168.200.1

Nom :    firewall.tpe.chartreux
Address:  192.168.200.2
```

```
C:\>nslookup 192.168.200.2
Serveur :  netserver.tpe.chartreux
Address:  192.168.200.1

Nom :    firewall.tpe.chartreux
Address:  192.168.200.2
```

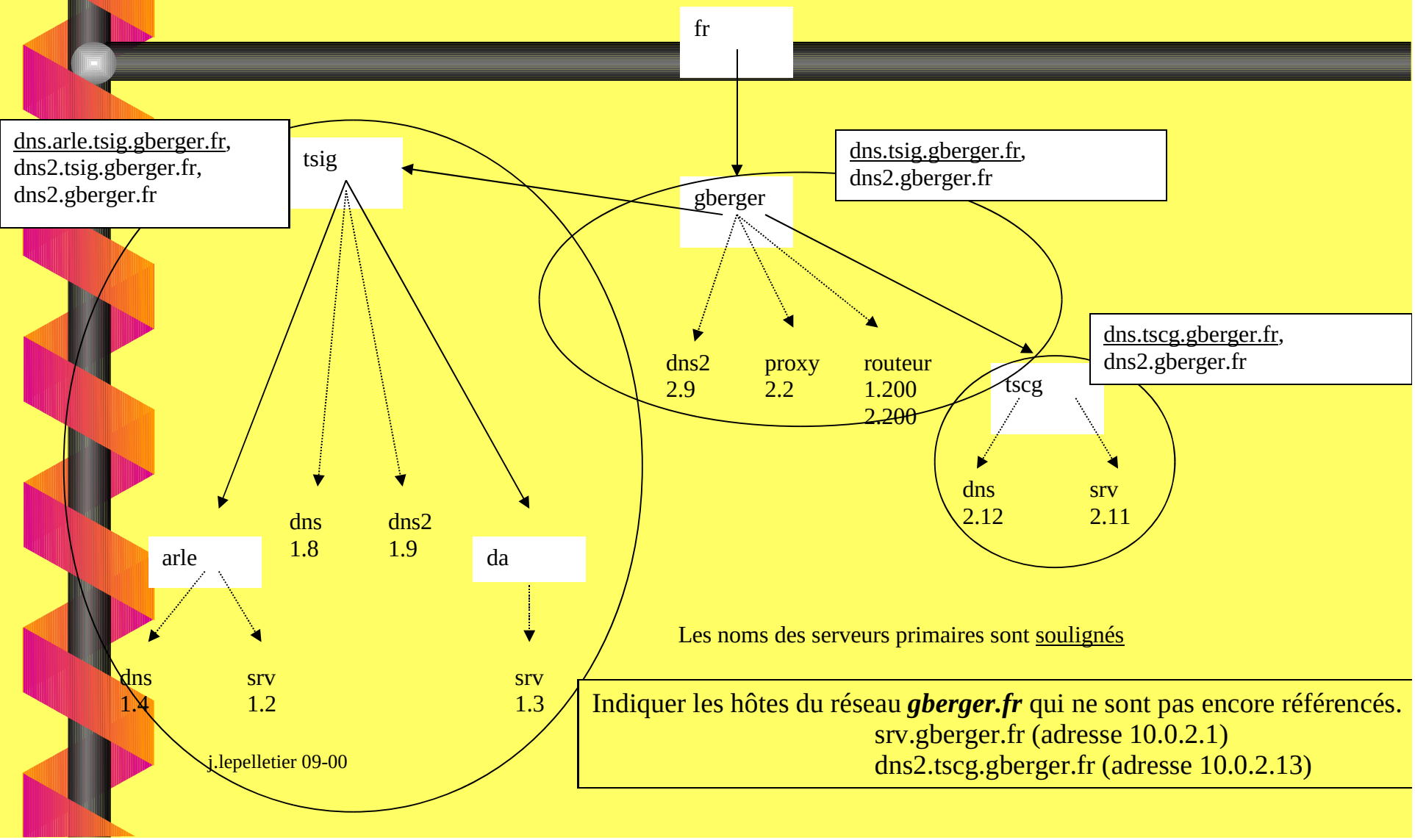
Exemple de nslookup



EXERCICE

EXONET 58

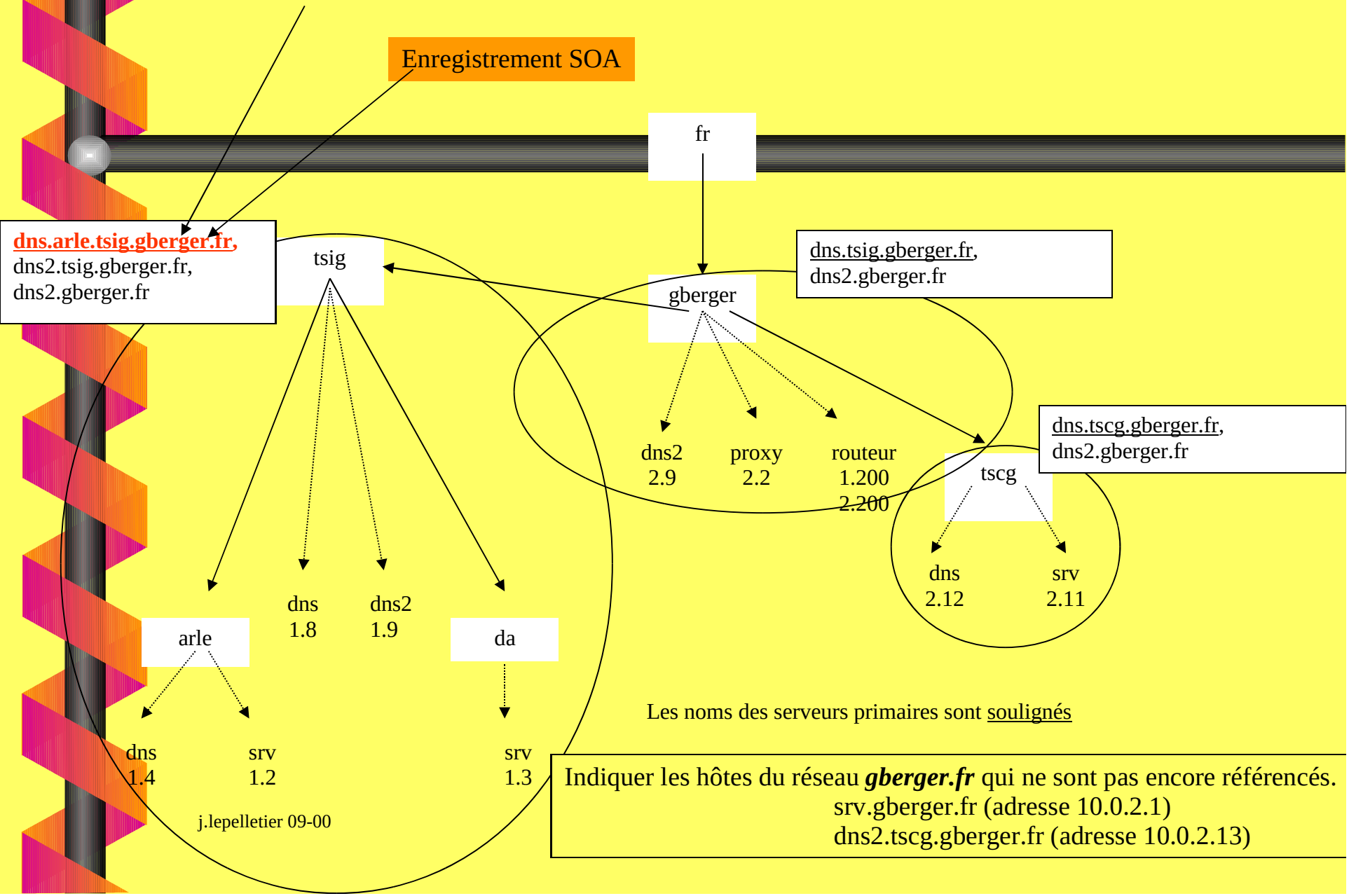
Compléter *l'annexe 3* afin de positionner chaque machine référencée dans son domaine (associée à son adresse IP) à partir de l'analyse du fichier de configuration des zones ***gberger.fr, tsig.gberger.fr*** *et* ***tscg.gberger.fr*** Faire apparaître pour chaque zone la liste des serveurs DNS.
Indiquer les hôtes du réseau ***gberger.fr*** qui ne sont pas encore référencés



Les noms des serveurs primaires sont soulignés

Indiquer les hôtes du réseau ***gberger.fr*** qui ne sont pas encore référencés.
srv.gberger.fr (adresse 10.0.2.1)
dns2.tscg.gberger.fr (adresse 10.0.2.13)

Sur quelle machine est stocké le fichier de configuration de la zone ***tsig.gberger.fr*** ?



Indiquer les hôtes du réseau ***gberger.fr*** qui ne sont pas encore référencés.

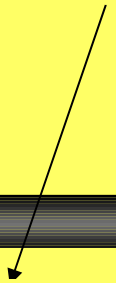
srv.gberger.fr (adresse 10.0.2.1)

dns2.tscg.gberger.fr (adresse 10.0.2.13)

Quelle est la durée de validité de ses données en cache (exprimée en jours) ?
Quelle est l'adresse et le nom du serveur secondaire de la zone *tscg.gberger.fr* ?

```
gberger.fr.   IN          SOA     dns.tsig.gberger.fr.   admgb.gberger.fr. (
3 ; numéro de version : permet aux serveurs secondaires de savoir s'ils doivent mettre à jour leur
base
36000         ; délai de mise à jour imposé aux serveurs secondaires (en secondes)
3600          ; délai avant une autre tentative de mise à jour par un serveur secondaire (en
secondes)
360000   ; durée au-delà de laquelle les données de zones seront marquées comme obsolètes par
un
serveur secondaire (en secondes)
86400); durée de validité en cache par défaut des enregistrements de zones (en secondes)

                          NS   dns.tsig.gberger.fr.
                          NS   dns2.gberger.fr.

tsig.gberger.fr.  IN      NS   dns.arle.tsig.gberger.fr.
                          NS   dns2.tsig.gberger.fr
                          NS   dns2.gberger.fr.

tscg.gberger.fr.  IN      NS   dns.tscg.gberger.fr.
                          NS   dns2.gberger.fr.

localhost.gberger.fr.           IN      A       127.0.0.1
dns2.gberger.fr.                IN      A       10.0.2.9
proxy.gberger.fr.               IN      A       10.0.2.2
routeur.gberger.fr              IN      A       10.0.2.200
routeur.gberger.fr              IN      A       10.0.1.200

; fin de la zone d'autorité
```

Parmi ces deux zones (***tsig.gberger.fr et tscg.gberger.fr***), quelle est la zone qui a é



tsig.gberger.fr. IN SOA dns.arle.tsig.gberger.fr. admig.gberger.fr. (**19** 18000 3600 72000 86400)
NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.
NS dns2.gberger.fr.

; délégation de la zone arle.tsig.gberger.fr avec deux serveurs

arle.tsig.gberger.fr. NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.

localhost.tsig.gberger.fr.		IN	A	127.0.0.1	
dns2.tsig.gberger.fr.	IN	A	10.0.1.9		***; adresse deuxième serv***
srv.da.tsig.gberger.fr.	IN	A	10.0.1.3		
srv.arle.tsig.gberger.fr.	***IN***	***A***	***10.0.1.2***		***; ligne à supprimer***

dns.arle.tsig.gberger.fr. IN A 10.0.1.4 ***; adresse premier serveur***

arle.tsig.gberger.fr est-elle une zone indépendante ?

non, car il n'y a pas de délégation de zone prévue , ni ***dans gberger.fr,*** ni dans ***tsig.gberger.fr***

Que faut-il faire pour que la résolution de nom pour la machine ***srv.gberger.fr***, d'adresse 10.0.2.1 soit possible ?

```
gberger.fr.   IN        SOA    dns.tsig.gberger.fr.   admgb.gberger.fr. (
);
                                NS   dns.tsig.gberger.fr.
                                NS   dns2.gberger.fr.


localhost.gberger.fr.           IN        A        127.0.0.1
dns2.gberger.fr.                IN        A        10.0.2.9
proxy.gberger.fr.               IN        A        10.0.2.2
routeur.gberger.fr              IN        A        10.0.2.200
routeur.gberger.fr              IN        A        10.0.1.200

Srv.gberger.fr                  IN        A        10.0.2.1
```

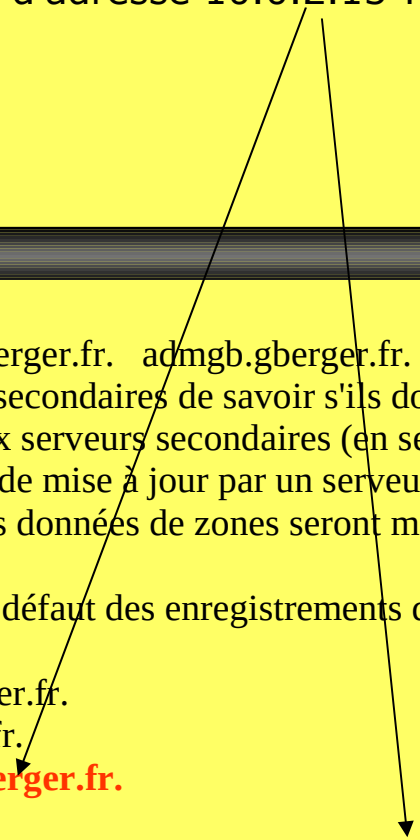
Quel est le contenu du fichier de description de zone associé au serveur ***dns2.tsig.gberger.fr***

Serveur secondaire

tsig.gberger.fr.	IN	SOA	dns.arle.tsig.gberger.fr.	admig.gberger.fr. (19 18000 3600 72000 86400)
		NS	dns.arle.tsig.gberger.fr.	
		NS	dns2.tsig.gberger.fr.	
		NS	dns2.gberger.fr.	
localhost.tsig.gberger.fr.		IN	A	127.0.0.1
dns.arle.tsig.gberger.fr.	IN	A	10.0.1.4	
dns2.tsig.gberger.fr.	IN	A	10.0.1.9	
srv.arle.tsig.gberger.fr.	IN	A	10.0.1.2	
srv.da.tsig.gberger.fr.	IN	A	10.0.1.3	

Description de la zone tsig

Comment faire pour déclarer un nouveau serveur secondaire pour la zone ***tscg.gberger.fr***, de nom ***dns2*** et d'adresse 10.0.2.13 ?



gberger.fr. IN SOA dns.tsig.gberger.fr. admgb.gberger.fr. (
3 ; numéro de version : permet aux serveurs secondaires de savoir s'ils doivent mettre à jour leur base
36000 ; délai de mise à jour imposé aux serveurs secondaires (en secondes)
3600 ; délai avant une autre tentative de mise à jour par un serveur secondaire (en secondes)
360000 ; durée au-delà de laquelle les données de zones seront marquées comme obsolètes par un serveur secondaire (en secondes)
86400); durée de validité en cache par défaut des enregistrements de zones (en secondes)

NS dns.tsig.gberger.fr.
NS dns2.gberger.fr.
NS dns2..tscg.gberger.fr.

tsig.gberger.fr. IN NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr
NS dns2.gberger.fr.

tscg.gberger.fr. IN NS dns.tscg.gberger.fr.
NS dns2.gberger.fr.

dns2.tscg.gberger.fr. IN A 10.0.2.13

Comment faire pour que ***arle.tsig.gberger.fr*** devienne une zone indépendante ?

créer une délégation de zone dans le fichier de configuration de tsig.gberger.fr

Contenu du fichier de configuration de la zone tsig.gberger.fr

tsig.gberger.fr. IN SOA dns.arle.tsig.gberger.fr. admig.gberger.fr. (19 18000 3600 72000 86400)
NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.
NS dns2.gberger.fr.

; délégation de la zone arle.tsig.gberger.fr avec deux serveurs

arle.tsig.gberger.fr. NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.

Contenu du fichier de configuration de la zone tsig.gberger.fr

tsig.gberger.fr. IN SOA dns.arle.tsig.gberger.fr. admig.gberger.fr. (19 18000 3600 72000 86400)
NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.
NS dns2.gberger.fr.

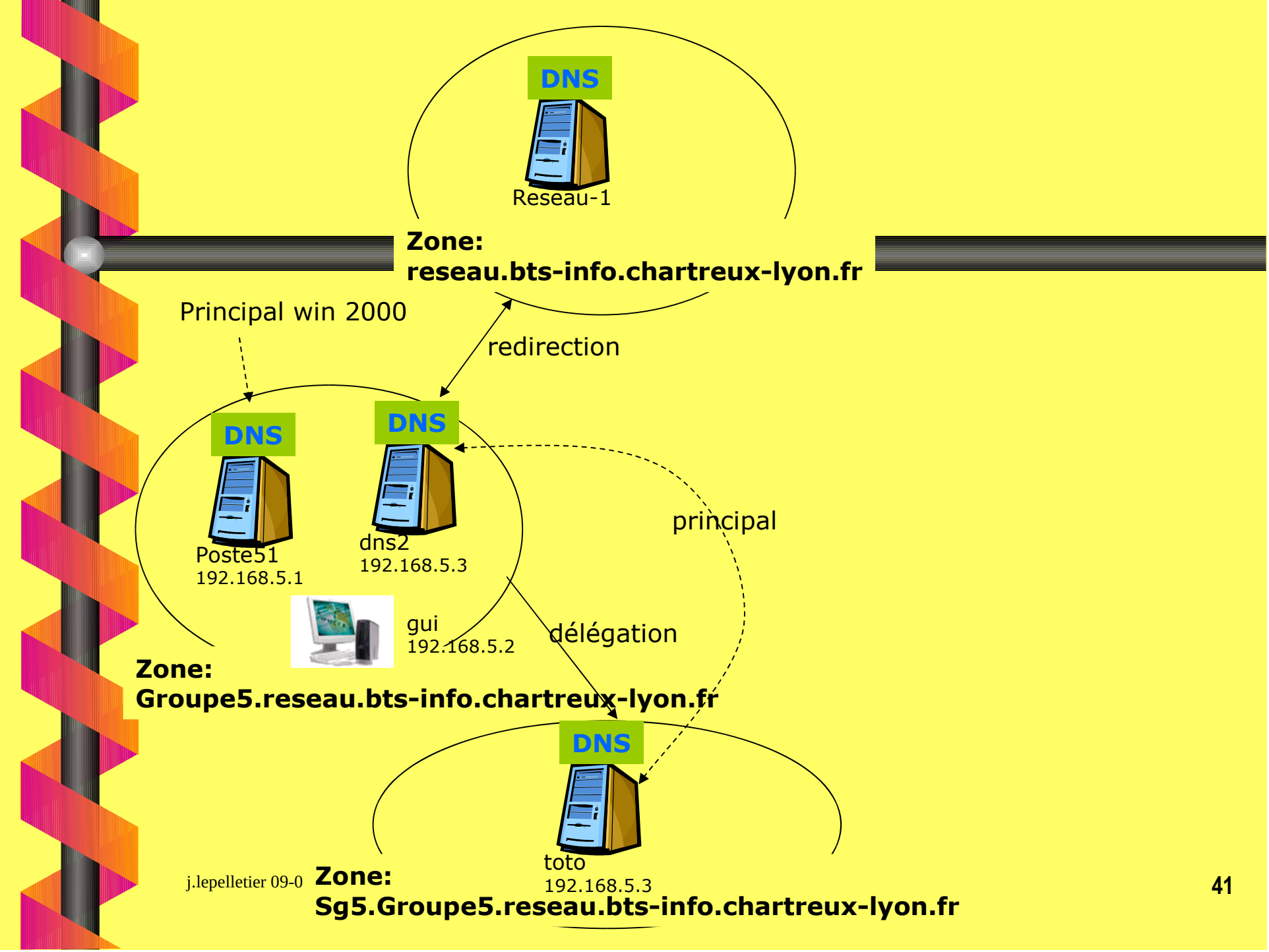
; délégation de la zone arle.tsig.gberger.fr avec deux serveurs

arle.tsig.gberger.fr. NS dns.arle.tsig.gberger.fr.
NS dns2.tsig.gberger.fr.

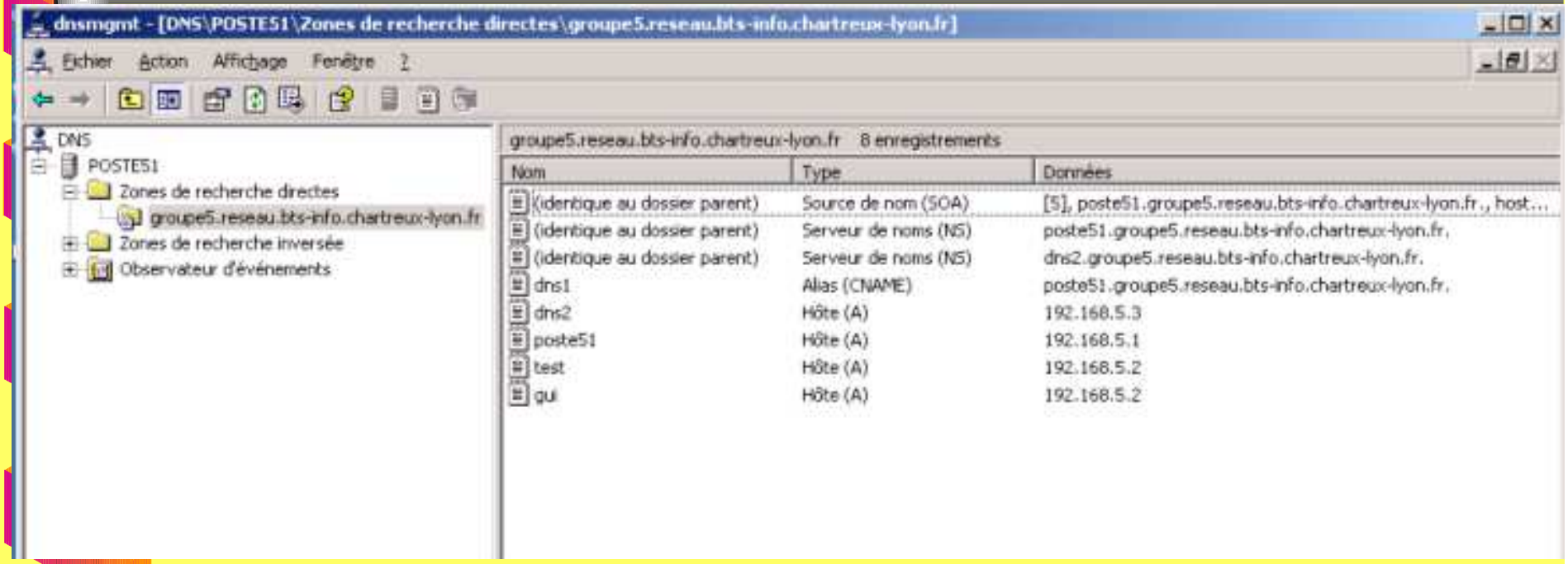
localhost.tsig.gberger.fr. IN A 127.0.0.1
dns2.tsig.gberger.fr. IN A 10.0.1.9 ***; adresse deuxième se***
srv.da.tsig.gberger.fr. IN A 10.0.1.3
srv.arle.tsig.gberger.fr. IN A 10.0.1.2 ; ligne à supprimer

; "glue data"

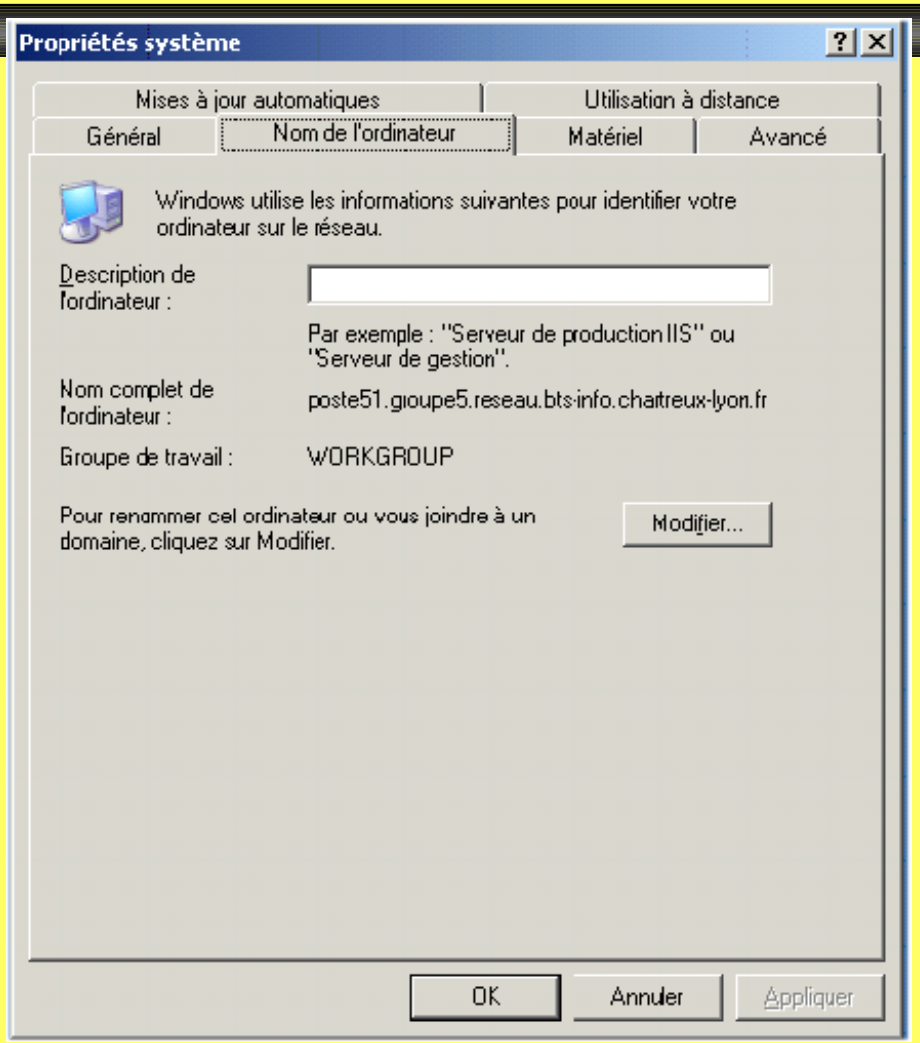
dns.arle.tsig.gberger.fr. IN A 10.0.1.4 ***; adresse premier serveur***


DNS
Reseau-1
Zone:
reseau.bts-info.chartreux-lyon.fr
Principal win 2000
redirection
DNS
DNS
Poste51
192.168.5.1
dns2
192.168.5.3
principal
gui
192.168.5.2
délégation
Zone:
Groupe5.reseau.bts-info.chartreux-lyon.fr
DNS
toto
192.168.5.3
Zone:
Sg5.Groupe5.reseau.bts-info.chartreux-lyon.fr

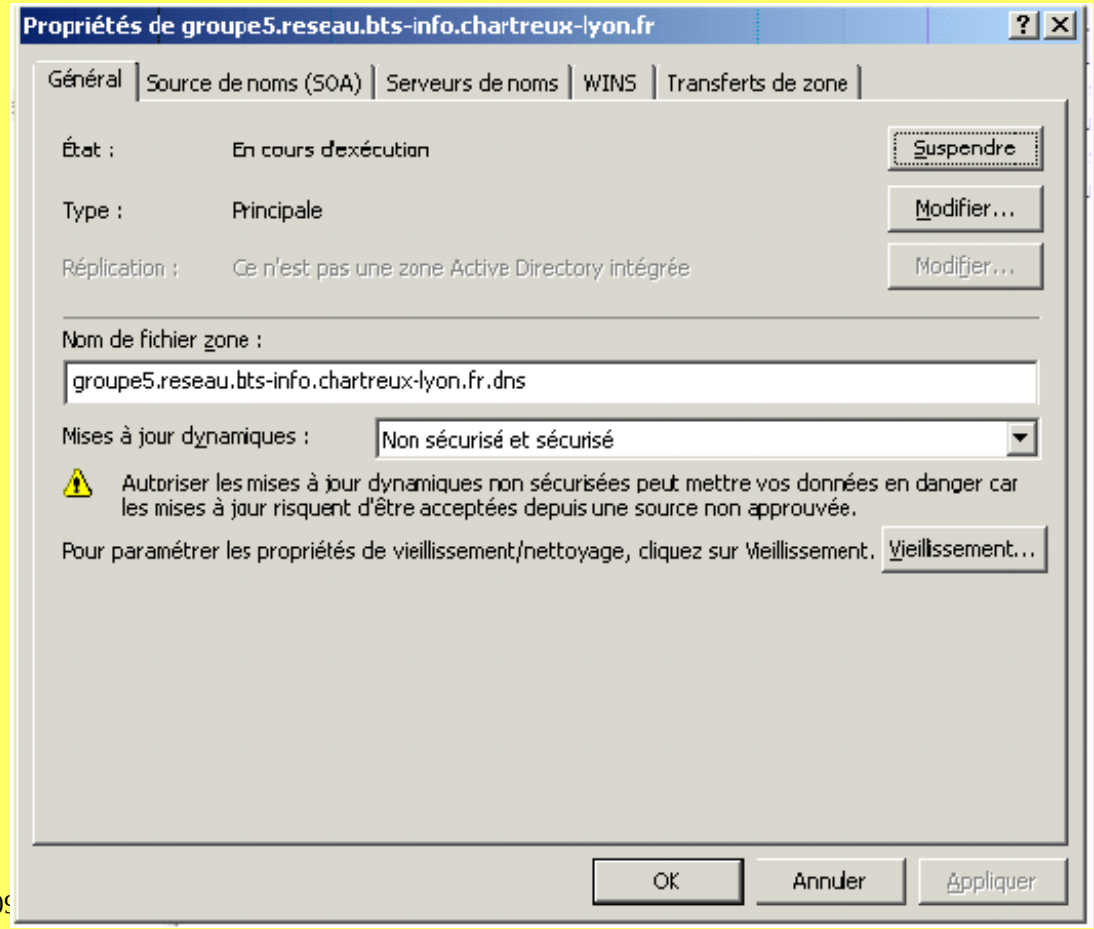
Création de la zone principale



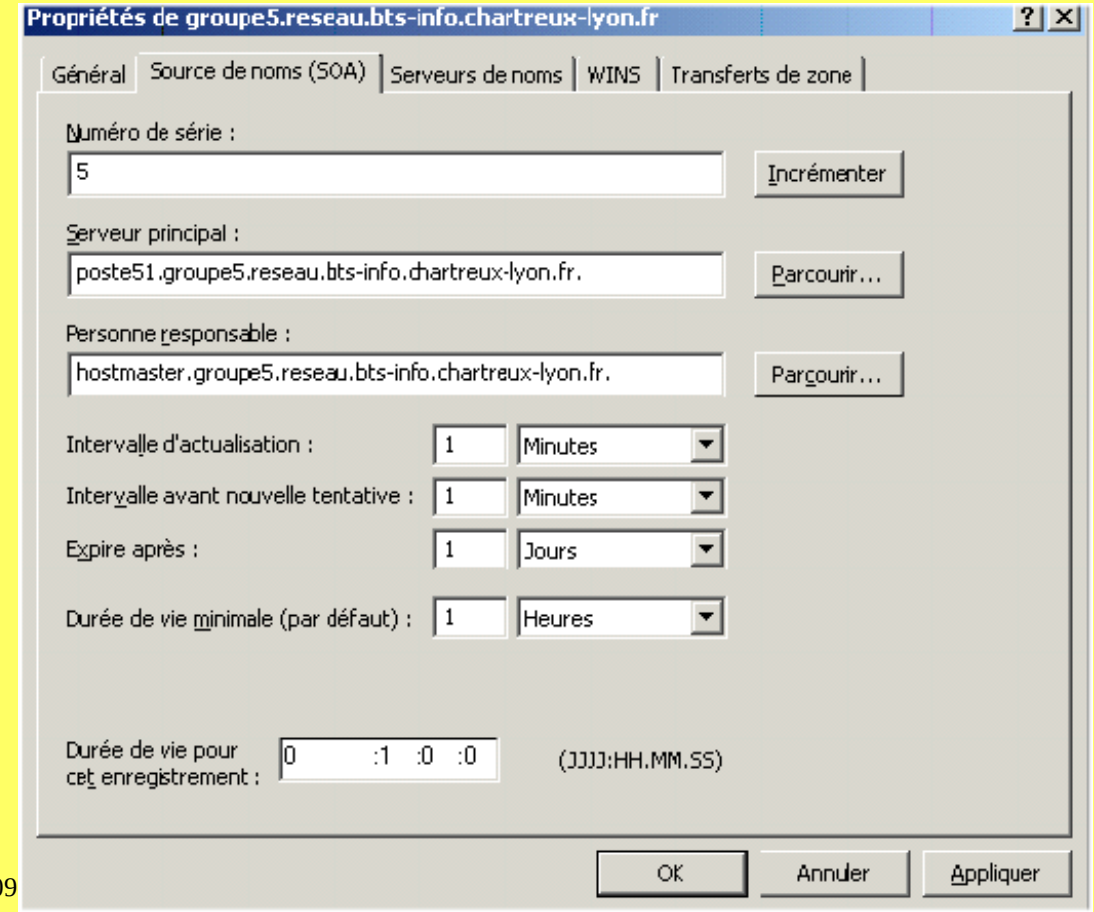
Définition du nom du serveur DNS



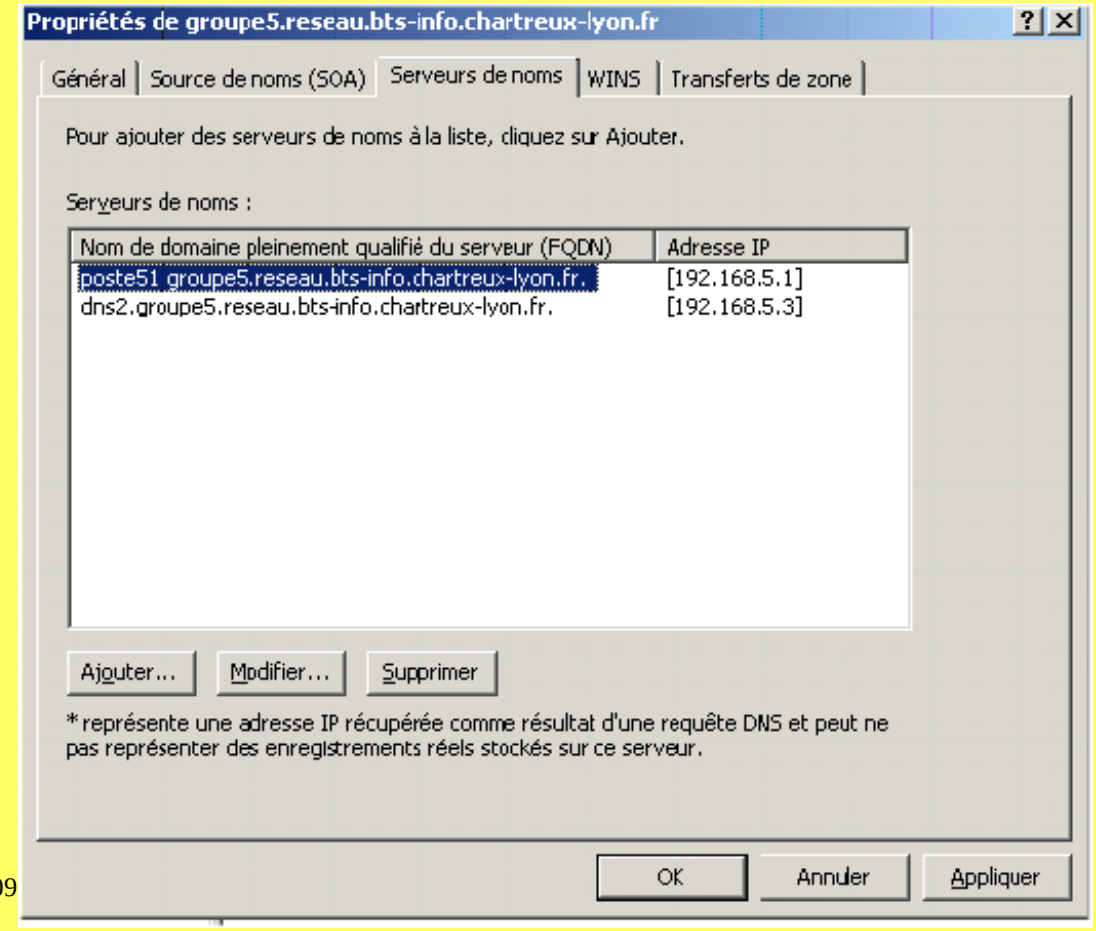
Descripti$ on de la zone principale



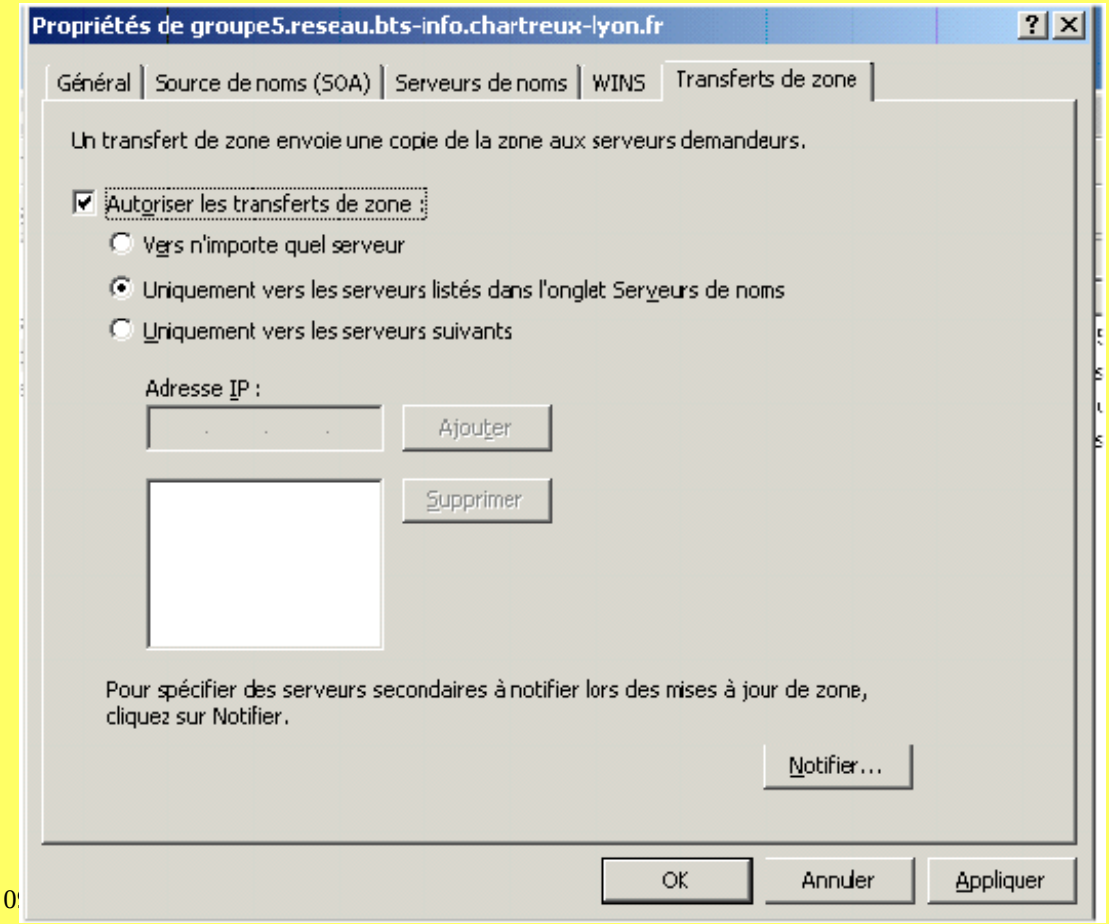
Description de la zone principale



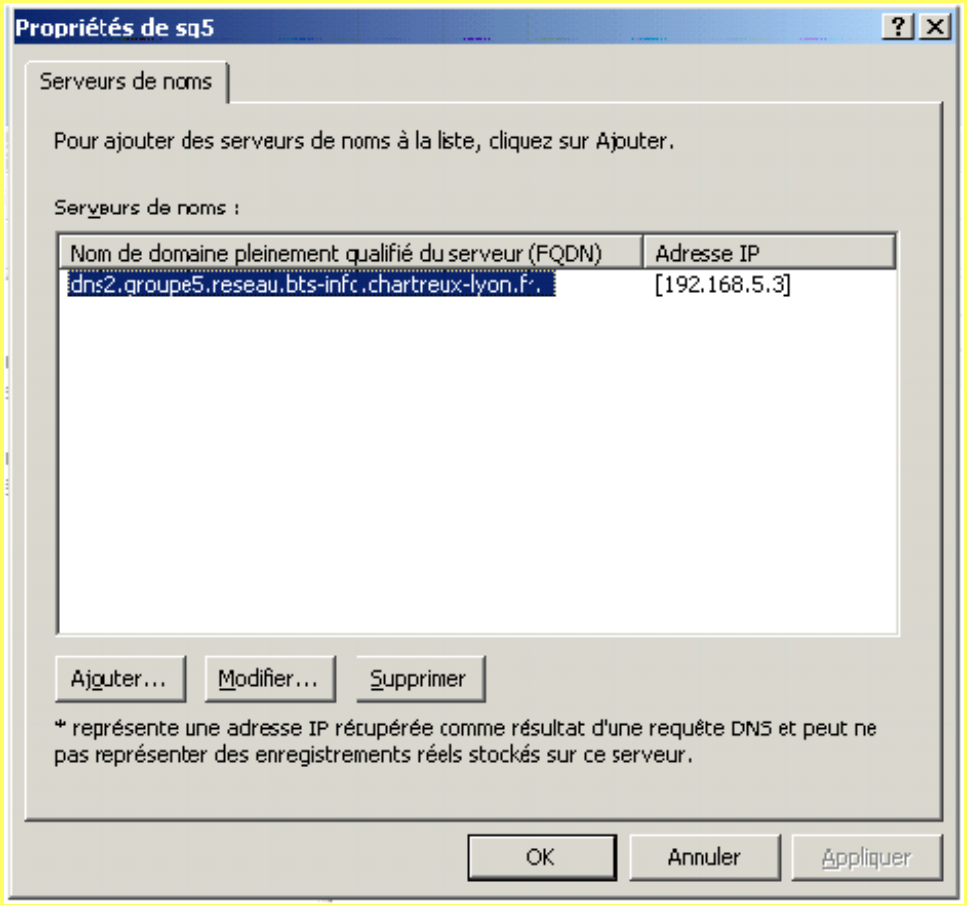
Description de la zone principale



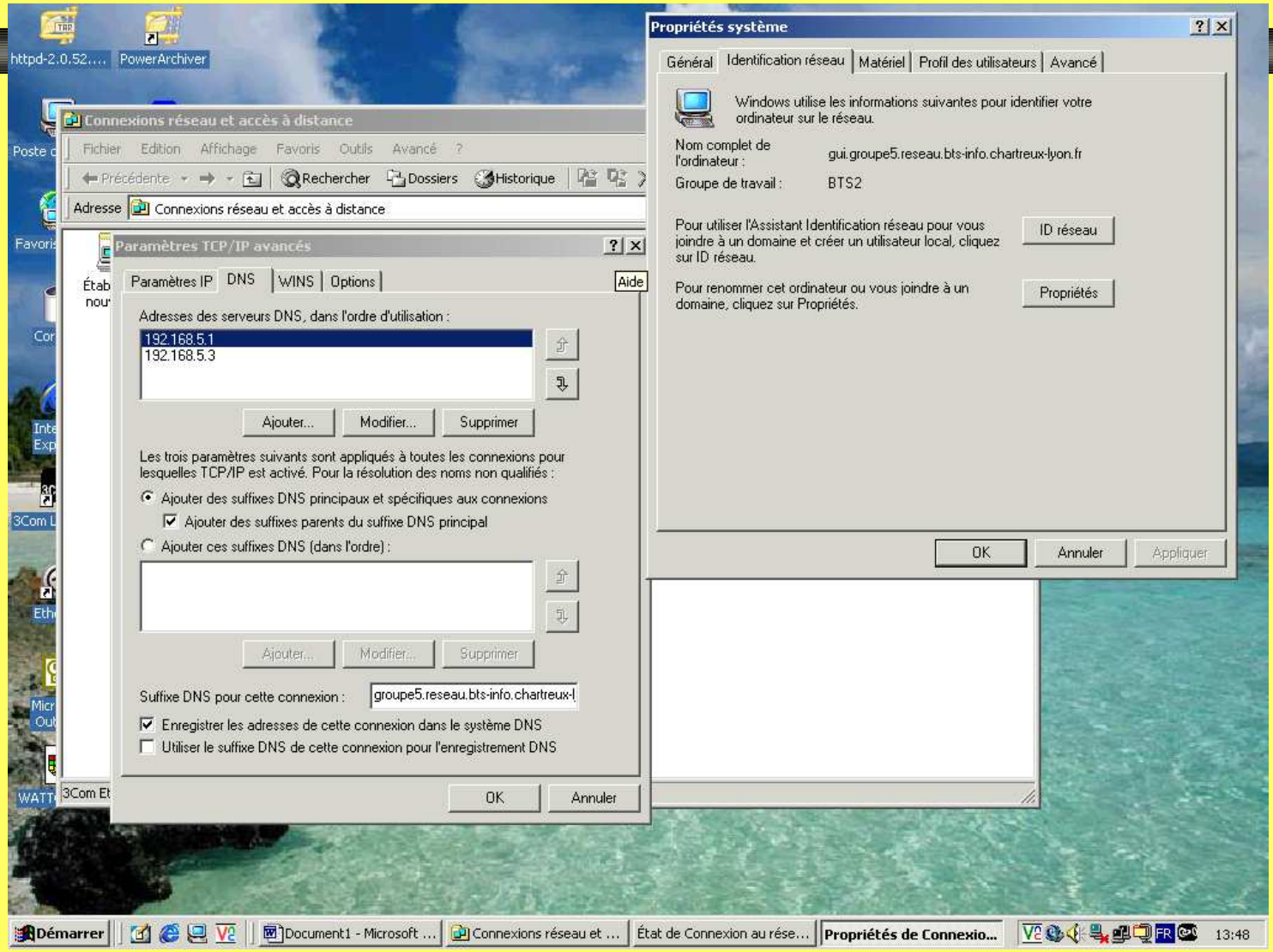
Description de la zone principale



Description du serveur second

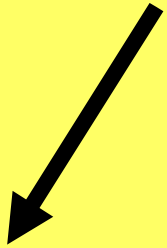


Client de la zone principale



DNS secondaire (linux)

Création d'une zone esclave sur le DNS secondaire



Named.conf:

```
Zone « groupe5.reseau.bts-info.chartreux-lyon.fr » {
        type slave;
        file « /var/named/groupe5.slave »;
        master {
                192.168.5.1;
                };
        };
```

Fichier maj par le primaire

/var/named/groupe5.slave

```
$ORIGIN .
$TTL 3600;  1 heure
groupe5.reseau.bts-info.chartreux-lyon.fr IN SOA
                                    groupe5.reseau.bts-info.chartreux-lyon.fr.
                                    (    les options
                                                    )
            NS dns2.groupe5.reseau.bts-info.chartreux-lyon.fr
            NS poste51. groupe5.reseau.bts-info.chartreux-lyon.fr

$ORIGIN groupe5.reseau.bts-info.chartreux-lyon.fr.
Dns1        CNAME     poste51
Dns2        A         192.168.5.3
Gui         A         192.168.5.2
Poste51     A         192.168.5.1
Test        A         192.168.5.2
```

Pour déléguer une zone

Créer une zone principale sur un serveur DNS appartenant à celle-ci (quelque soit l'adresse IP)

Déléguer cette zone (nouvelle délégation)