17

La gestion des noms

Partie de la câblerie et de la basse filasse, nous abordons dans ce chapitre les couches applicatives, c'est-à-dire les services réseau. Pour ainsi dire, nous nous élevons dans les couches supérieures du réseau.

Car, de nos jours, l'administrateur réseau ne peut pas se contenter de fournir le transport des données. Il doit en faciliter l'accès à ses utilisateurs.

En outre, plus le nombre d'utilisateurs est élevé, plus il est important de simplifier les tâches administratives.

Il convient donc d'utiliser des outils qui simplifient la vie des utilisateurs et celle des exploitants. Le service de nom, ou DNS (*Domain Name System*), est le premier d'entre eux.

Dans ce chapitre vous apprendrez ainsi :

- à comprendre le fonctionnement du DNS ;
- à définir un plan de nommage ;
- à configurer les serveurs DNS ;
- à configurer les PC ;
- à interroger la base de données du DNS.

Présentation du DNS

Pour vos utilisateurs et vous-même, il serait bien plus pratique d'utiliser des noms de machines plutôt que des adresses, à l'instar de ce qui se fait sur l'Internet. De même que l'on accède à www.3com.com, il serait bien plus simple d'accéder à votre serveur au moyen du nom www.societe.fr plutôt que de son adresse IP.

La première solution repose sur l'utilisation des fichiers hosts (localisés dans /etc sous Unix, et dans \Windows sous Windows 9x). Ce fichier contient simplement la correspondance entre adresses IP et noms de machines :

```
10.0.0.1      par001
10.0.0.100    nt001
10.0.0.101    mail
```

L'inconvénient de cette méthode est qu'il faut configurer le fichier sur chaque poste de travail, et ce, à chaque changement d'adresse ou de nom. On pourrait imaginer une distribution automatique de ce fichier, mais cette opération serait très complexe et source d'erreur avec les PC. De plus, l'espace de nommage est " plat " (tous les noms sont au même niveau).

La seconde solution, de loin la meilleure, repose donc sur l'utilisation d'un système DNS (*Domain Name System*). C'est celle utilisée à grande échelle sur l'Internet (plusieurs millions de machines référencées début 2001) et qui convient également pour vos 10 ou 10 000 PC.

Les composants du DNS

Le DNS a déjà été introduit aux chapitres 3, 15 et 16 lorsque, par exemple, nous nous sommes promenés sur l'Internet. Il s'agit ici de recréer un DNS privé, c'est-à-dire réservé à nos utilisateurs.

Il faut pour cela définir :

- un espace de nommage hiérarchique découpé en domaines ;
- des serveurs gérant des bases de données ;
- des clients appelés *resolver* ;
- un protocole d'échange entre clients et serveurs d'une part, et entre serveurs d'autre part.

Tous ces composants sont décrits dans une série de RFC dont les premiers remontent à 1987.

Élaborer un plan de nommage

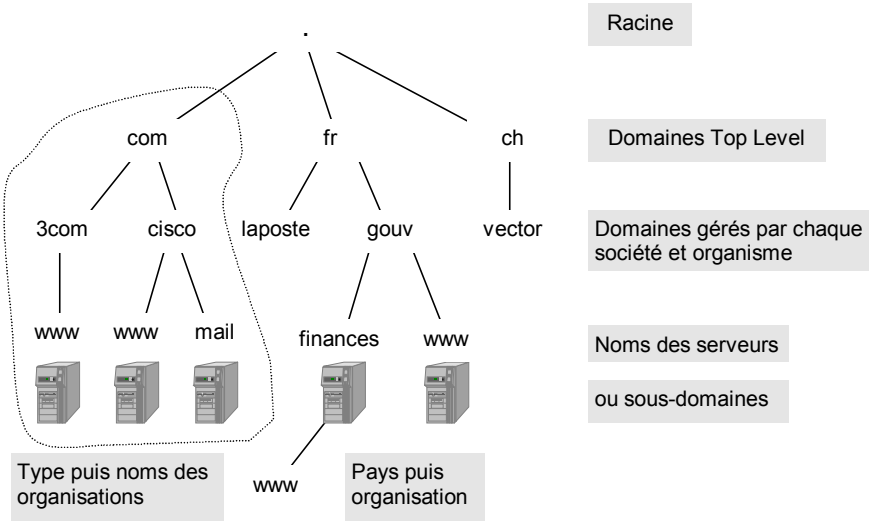
Le nommage DNS est organisé sous forme d'arbre, avec une racine et des domaines qui lui sont rattachés. Le plan de nommage consiste donc à définir cette arborescence et la manière d'affecter des noms aux objets (les feuilles de l'arbre).

Définir l'arborescence DNS

Dès le début de votre réflexion, vous serez confronté au dilemme classique : définir une arborescence qui reflète l'organisation de la société ou une arborescence qui reflète son implémentation géographique ?

Par expérience, l'une n'est pas meilleure que l'autre, car toutes deux sont soumises aux aléas des changements. L'approche organisationnelle est soumise au changement du nom de la société (suite à une décision stratégique, à un rachat, etc.) ou du service (suite à une réorganisation), tandis que l'approche géographique est soumise aux déménagements.

L'Internet a d'ailleurs retenu les deux approches.



Pour notre DNS privé, donc à usage purement interne, nous n'avons pas besoin de faire référence au pays et au nom de la société, mais plutôt à la ville, au nom du site et au nom des directions (ou, selon la terminologie propre à chaque société, des divisions, des *Business Units*, etc.).

Nous pouvons cependant retenir la même approche mixte en fonction du degré de centralisation de chaque département.

Représentation dans le DNS	Organisation centralisée	Organisation décentralisée
Racine	Par convention, le point ('.')	Par convention, le point ('.')
Domaine Top Level	Nom de la direction	Nom de la ville
Domaine (optionnel)	Nom de la ville	Nom de la direction

Il est conseillé de ne retenir que les invariants ou, pour être exact, les éléments qui sont susceptibles de changer le moins souvent. Dans notre cas, ce sont les directions (c'est-à-dire les services situés au sommet de la hiérarchie organisationnelle) et les villes principales où est implantée notre société.

L'espace de nommage est indépendant de la localisation géographique : tous les immeubles d'une même ville peuvent donc être référencés dans le même domaine DNS.

Par exemple, l'indication d'éléments pouvant changer fréquemment, tels que le nom du service au sein d'une direction ou le nom du site dans une ville, est source de complication, et entraîne un travail supplémentaire de reconfiguration. Plus vous ajouterez de niveaux au DNS, plus vous devrez effectuer de mises à jour. En revanche, si un service au sein d'une direction devait garder son autonomie, on pourrait envisager de lui déléguer la gestion de son sous-domaine.

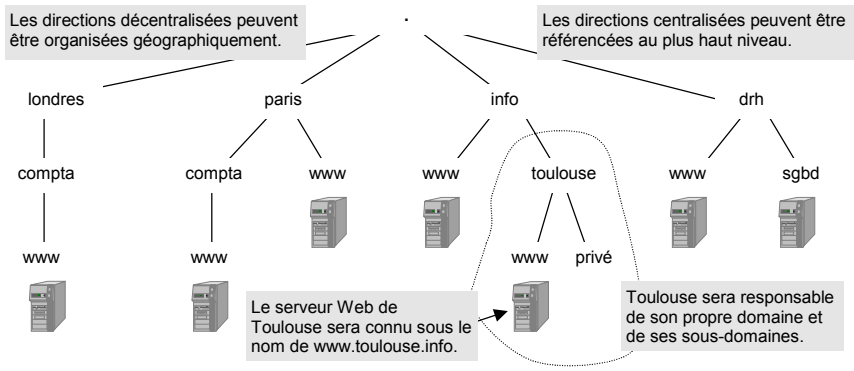


Figure 17-1. *Définition d'un DNS privé.*

Le DNS offre donc beaucoup de souplesse :

- Une même machine (ayant une adresse IP) peut être référencée dans plusieurs domaines.
- Une même machine peut être référencée sous plusieurs noms principaux et/ou sous un nom principal associé à des alias.
- La gestion d'un domaine peut être déléguée à un nouveau service devenu autonome, ou être reprise de façon centrale.
- Une direction peut gérer son propre DNS (avec sa propre racine).
- Les machines peuvent être référencées dans plusieurs DNS.
- Un DNS peut comporter une centaine de niveaux.

On le voit, le DNS permet toutes sortes de fantaisies. Il est donc de votre responsabilité d'en assurer la cohérence et la simplicité. Ainsi, les fonctionnalités présentées ci-dessus doivent-elles plutôt être utilisées pour faciliter les périodes de transition lors de changements d'organisation ou de déménagement ou, d'une manière générale, pour répondre à des situations exceptionnelles.

Standardiser le nommage des objets

Il n'est pas nécessaire de mettre les postes de travail dans la base DNS, car ces derniers ne sont que des clients ; ils ne sont pas connus en tant que serveur. Seuls sont renseignés dans les bases DNS les équipements réseau (pour les exploitants) et les serveurs (pour les utilisateurs).

Il est conseillé d'adopter un codage différent et adapté à chaque type d'objet, c'est-à-dire à sa nature et à sa fonction. Par exemple, les serveurs ne seront pas nommés de la même manière que les routeurs. Le nom principal doit correspondre à un invariant, et les alias à la particularité du moment.

Si la sécurité est privilégiée et que le nom ne doit pas permettre d'identifier ces éléments, des noms neutres peuvent être retenus (noms de musiciens, de fleurs, de planètes, etc.).

Objet	Invariant	Variant
Serveur	Système d'exploitation (Unix, NT)	Fonction (web, messagerie, base de donnée, etc.)
Routeur	Marque (Cisco, 3com, etc.) et fonction de routage	Localisation
Concentrateur	Marque (3com, etc.) et fonction de concentration	Localisation et, éventuellement, emploi de réseaux différents (Ethernet, ATM, etc.)
Commutateur	Marque (Cisco, 3com, etc.) et fonction de commutation	Localisation et, éventuellement, emploi de réseaux différents (Ethernet, ATM, etc.)
Serveur d'accès distant	Marque (Cisco, 3com, etc.) et fonction d'accès distant	Localisation

La localisation peut être considérée comme étant un variant de faible impact à partir du moment où l'équipement doit de toute façon être reconfiguré (changement d'adresse IP, par exemple).

Il faut privilégier un nommage simple des équipements auxquels on accède le plus fréquemment : les serveurs (auxquels accèdent les utilisateurs) et les routeurs et serveurs d'accès distants (auxquels accèdent les exploitants réseau). Le nom doit :

- Ne comporter que des caractères alphanumériques (minuscules et/ou majuscules) et des tirets (-). Ils constituent, en effet, le plus petit dénominateur commun dans le monde de l'informatique. Les autres caractères sont à proscrire, car certains systèmes ne les acceptent pas.
- Être court, afin d'être facile à mémoriser et rapide à saisir au clavier.
- Contenir une ou deux alternances de noms et de chiffres pour en améliorer la lisibilité.
- Contenir un tiret au maximum pour séparer deux champs alphabétiques ou numériques, afin d'en améliorer la lisibilité.

Équipement	Codage retenu	Nom principal (nom système)	Exemple
Serveur NT	Nom neutre (planètes)	mars pluton	mars.marseille. mars.paris.
Unix	Nom neutre (musiciens)	mozart schubert	mozart.toulouse.info.
Routeur	Ville sur trois lettres et numéro d'ordre sur trois chiffres	par001, par002 toul001	par001.info. par001.paris.
Serveurs d'accès distants	Préfixe svc, suivi du codage identique aux routeurs	ras-par001 ras-mar002	ras-mar002.info.

Un serveur peut être connu sous plusieurs noms :

- Un premier qui désigne sa nature et qui correspond au nom système défini lors de l'installation. Il ne change pas (sauf lors d'une réinstallation).
- Un ou plusieurs autres qui désignent sa ou ses fonctions et qui correspondent à une ou plusieurs applications (base de donnée, web, etc.)

Pour les utilisateurs, le meilleur moyen d'identifier et de mémoriser le nom d'un serveur est de lui donner le nom de l'application dont ils se servent. Un **alias** correspondant à la fonction du serveur pourra donc être défini et correspondre à la fonction du serveur (il varie au cours du temps alors que le nom système ne change que si l'on réinstalle complètement la machine).

Fonction	Codage retenu	Alias	Exemple
Serveur web principal	Convention universelle	www	www.paris. www.toulouse.info. www.drh.
Autres serveurs web	Convention suivie d'un numéro d'ordre sur un chiffre	www1 www2	www.paris. www1.paris. www2 .paris.
Messagerie	Mail suivi d'un numéro d'ordre	mail mail1	mail.paris. mail1.info.
Autres applications	Nom de l'application	compta rivage	compta.paris. rivage.info.

Certains serveurs centraux, c'est-à-dire communs à l'ensemble de la société, pourront être situés juste sous la racine. On aura, par exemple, www pour le serveur servant de point d'entrée à toute la société : il contiendra les informations du jour et des liens vers les autres serveurs web. On pourra aussi y placer les serveurs qui réalisent l'interconnexion des messageries.

Les concentrateurs et les commutateurs ne sont généralement pas accessibles au moyen d'une connexion Telnet, mais *via* SNMP et une station d'administration. Le codage des noms peut donc être plus complexe. Il peut refléter leur localisation géographique et, éventuellement, leur fonction, afin de faciliter leur identification. Dans notre cas, nous avons choisi le codage suivant : [type]-[ville][étage][immeuble].

Champ	Signification	Code
[type]	Type de matériels, sur une lettre	**H** = Hub, **S** = switch, **A** = ATM, **F** = Frame Relay, **I** = FDDI
[ville]	Abréviation de la ville, sur trois lettres	**par** = Paris, **tou** = Toulouse **tur** = Tour, etc.
[immeuble]	Lettre majuscule identifiant un immeuble dans la ville	Le code dépend de la ville **D** = Descartes, **M** = Montparnasse, etc.

Ce qui donne, par exemple, h-par05a, s-tou05D, etc.

Afin de faciliter leur lecture et leur traitement dans des bases de données, il est préférable que chaque champ ait une longueur fixe.

Configurer les serveurs DNS

Le DNS est géré par des serveurs qui assurent plusieurs fonctions :

- la gestion d'une **zone**, c'est-à-dire d'un domaine et de ses sous-domaines : on dit que le serveur a **autorité** sur la zone ;
- l'échange des bases de données au sein d'une zone : un serveur est désigné **primaire** pour une zone et distribue la base de données aux serveurs **secondaires** ;
- le **relais** des requêtes DNS d'un client sur un nom situé dans une autre zone ;
- le **cache** des requêtes clients de manière à limiter les requêtes ;
- enfin, un serveur doit être désigné **racine** de l'arbre DNS.

Tout serveur DNS est serveur cache et peut être à la fois ou seulement :

- **primaire** pour un ou plusieurs domaines ;
- **secondaire** pour un ou plusieurs autres domaines ;
- **racine**.

Comme pour le nommage, le DNS offre de nombreuses possibilités et peu de contraintes :

- Il faut au moins un serveur racine.
- Il faut un et un seul serveur primaire par domaine.
- Toutes les modifications de la base de données d'une zone doivent être réalisées sur le serveur qui a autorité (le serveur primaire).

- Il peut y avoir aucun ou autant de serveurs secondaires par domaine.
- Les fonctions primaires et secondaires sont exclusives pour un domaine donné.
- Mais un serveur peut être à la fois primaire pour un domaine et secondaire pour un autre.
- Un serveur DNS peut ne servir que de cache (c'est-à-dire n'être ni racine, ni primaire, ni secondaire).
- L'administrateur peut déléguer la gestion d'un domaine faisant partie de la zone d'autorité à un autre serveur qui devient alors primaire pour le domaine.
- Les clients et les serveurs DNS peuvent être situés n'importe où sur le réseau : sur des lieux géographiques différents et sur des réseaux IP différents.
- Il peut y avoir plusieurs DNS distincts.
- Les postes de travail et les serveurs peuvent être référencés dans n'importe quel domaine.

Le DNS permet de faire tout et n'importe quoi. Il convient donc de respecter quelques règles afin de conserver une certaine cohérence au sein de votre société. Ainsi, vous devez prévoir :

- au moins un serveur DNS par site afin de ne pas surcharger les liaisons WAN ;
- au moins un serveur secondaire en partage de charge et en secours ;
- un arbre DNS pour toute la société, même si chacun gère son propre domaine.

Les bonnes pratiques du DNS sont exposées dans la RFC 1912.

Selon ces principes, nous avons décidé de créer l'architecture présentée ci-après.

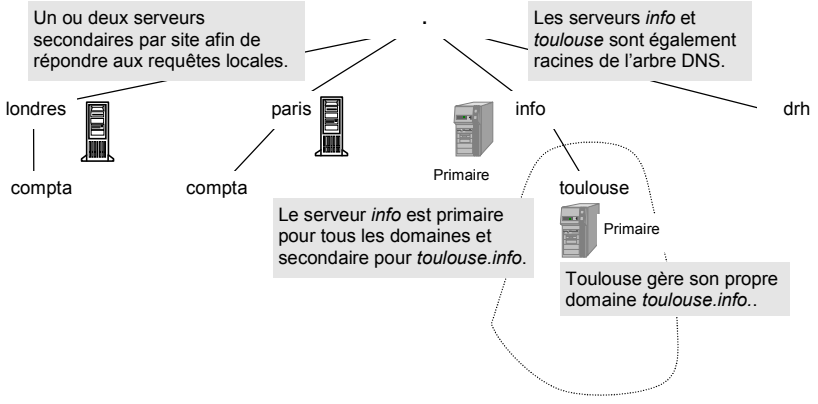


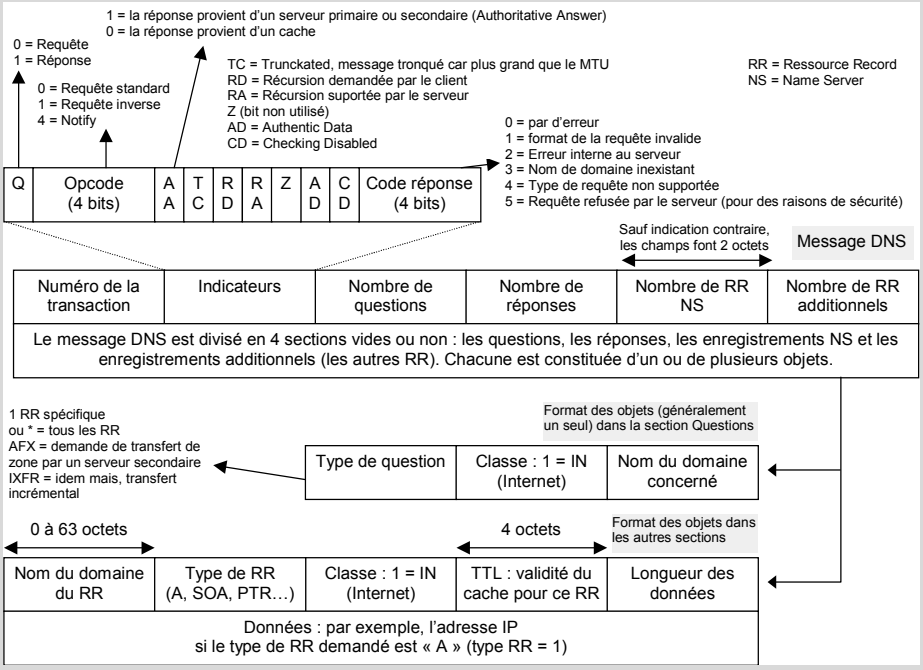
Figure 17-2.
Les serveurs DNS.

Chaque serveur DNS gère une partie de la base de données DNS, celle représentant la zone sur laquelle il a autorité. Le serveur de Toulouse ne contiendra ainsi que les objets situés dans la zone " toulouse.info ".

Sous Windows NT, la manipulation de la base de données est réalisée à l'aide du Gestionnaire DNS, situé dans le menu " Démarrer → Programmes → Outils d'administration ". Celui-ci sauvegarde les données dans la base des registres Windows (clé \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \Dns) et maintient une copie sous forme de fichiers ASCII dans le répertoire \Winnt\System32\Dns. Ces fichiers respectent le format des serveurs DNS sous Unix, tels que ceux produits par la version appelée BIND et développée à Berkeley.

LE POINT SUR LE DNS (RFC 1034, 1035, 1995, 1996, 2181)

Le DNS (*Domain Name System*, quelquefois appelé *Domain Name Service*) définit une base de données découpée en **zones** (constituées d'un **domaine** et de ses sous-domaines) correspondant à une partie d'un **arbre hiérarchique**. Un serveur peut avoir autorité sur une ou plusieurs zones. S'il est **primaire**, il est maître de la zone. S'il est **secondaire**, il dispose d'une copie qu'il demande régulièrement au [serveur] primaire. S'il est **racine**, le serveur a autorité sur la racine de l'arbre. Les serveurs racines peuvent **déléguer leur autorité** aux serveurs gérant le premier niveau de domaines, appelés domaines **Top Level**, et ainsi de suite. Tous les serveurs font également office de **cache** pour les requêtes DNS émises par les clients appelés **resolver**.

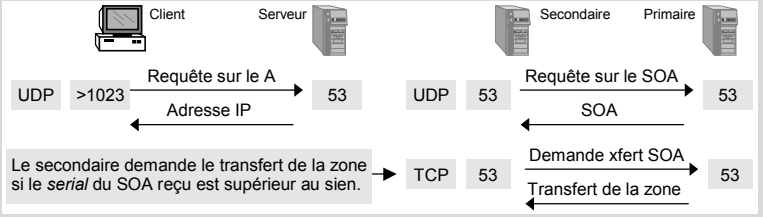


Afin de diminuer la taille des messages DNS, les noms apparaissant plusieurs fois peuvent être remplacés par des pointeurs de deux octets indiquant la position de l'unique exemplaire du nom.
La longueur maximale d'un nom d'objet est de 63 octets, et celle d'un nom de domaine complet (y compris celui de l'objet) est de 255 octets.

• • •

LE POINT SUR LE DNS (SUITE)

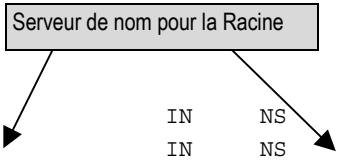
Les messages DNS transitent dans des paquets UDP ou TCP selon les cas (port 53).



Le RFC 1995 précise un mode de transfert incrémental (seules les modifications sont transférées). Le RFC 1996 spécifie, quant à lui, un mécanisme permettant au primaire de notifier au secondaire que le SOA vient d'être modifié. Cela évite d'attendre la fin de la période indiquée dans le paramètre *refresh*.

Configurer le fichier cache

Tous les serveurs participant à votre DNS doivent connaître les serveurs racines. Ces informations résident dans le **fichier cache** (attention, celui-ci n'a rien à voir avec le serveur appelé cache). Sous Windows NT, ce fichier est situé dans le répertoire \Winnt\System32\Dns\Cache.dns. Il doit être édité manuellement sur chaque serveur DNS de votre société :




```
.                    IN     NS     nt001.info.
.                    IN     NS     nt004.toulouse.info.
nt001.info.          IN     A      10.0.0.100
nt004.toulouse.info. IN     A      10.4.0.165
```

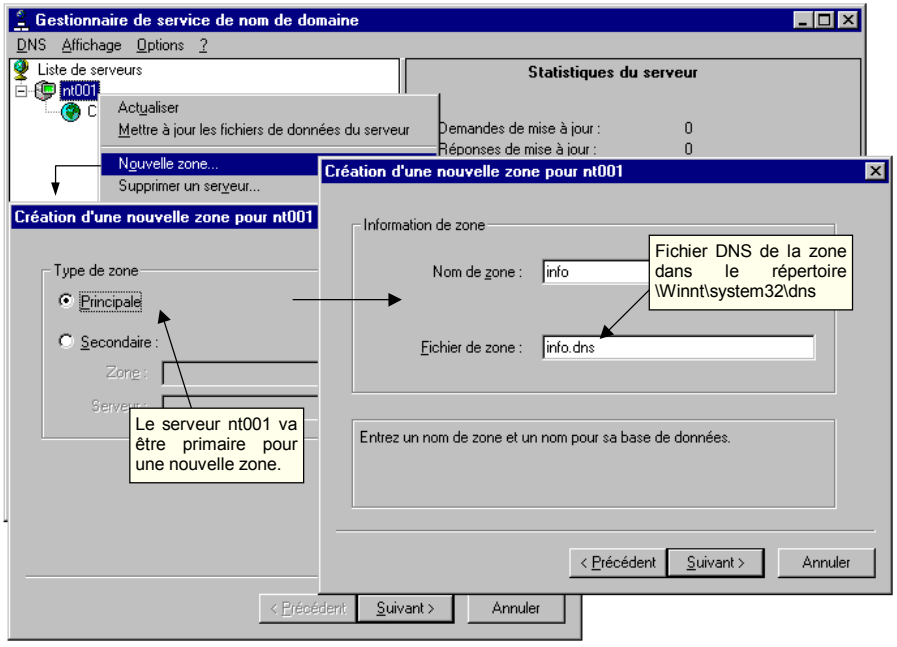
Les instructions NS (*Name Server*) et A (*Address*) indiquent les adresses IP des serveurs racines. Il peut y en avoir autant que nécessaire, afin d'assurer la redondance et le partage de charge.

Si vous voulez construire un DNS intranet directement rattaché à l'Internet, il faut y indiquer les serveurs racines officiels. (Vous pouvez vous procurer la dernière version sur le site ftp://ftp.rs.internic.net/domain/named.root.) Vous obtenez alors le fichier cache suivant (extrait) :

```
;
; formerly NS.INTERNIC.NET
;
.                        3600000   IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000       A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000       NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000       A     128.9.0.107
.........
```

Configurer un serveur primaire

Dans le DNS, il est nécessaire de configurer un serveur primaire unique pour chaque zone. Un serveur primaire pour une zone est primaire pour le domaine situé en tête de cette zone, ainsi que pour tous les sous-domaines.



Cela a pour effet de produire le fichier C:\Winnt\System32\Dns\info.dns :

```
;
;  Database file info.dns for info zone.
;       Zone version:  1
;
@                       IN  SOA nt001.info. administrateur.info. (
                                1           ; serial number
                                3600        ; refresh
                                600         ; retry
                                86400       ; expire
                                3600      ) ; minimum TTL

@                           NS  nt001
nt001                       A   10.0.0.100
nt004.toulouse              A   10.4.0.165
```

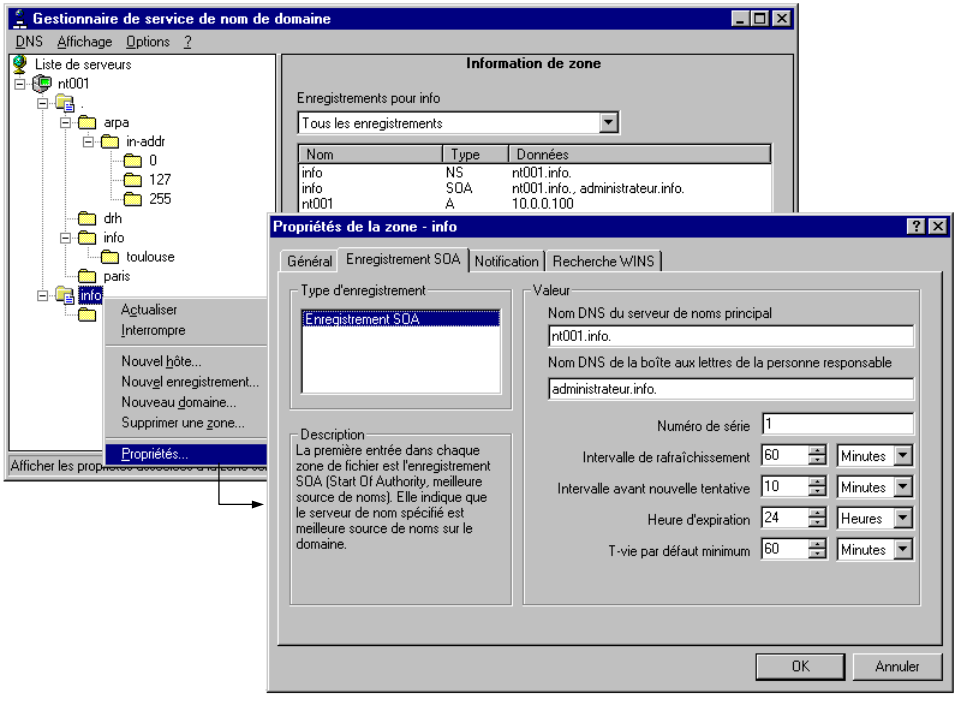
Les parenthèses doivent être utilisées si les paramètres tiennent sur plusieurs lignes.

Description de la zone info.

Référence relative à la zone en cours, ici " info. ".

Serveur primaire pour la zone en cours.

Que ce soit sous NT ou sous Unix, il est possible d'éditer manuellement ce fichier pour modifier les paramètres de la zone. Avec le gestionnaire DNS de Windows, on obtient l'écran suivant.



Les paramètres de la zone (SOA, *Start Of Authority*) sont définis au niveau du serveur primaire pour être ensuite utilisés par les serveurs secondaires. Le champ " Temps par défaut minimum " pourra également être utilisé par les resolvers pour déterminer la durée de conservation de l'enregistrement dans leur cache.

Si vous voulez limiter les échanges entre serveurs, mieux vaux positionner le paramètre " refresh " à une valeur assez élevée, généralement 12 à 24 heures, sauf durant les périodes de changement. En prévision de telles périodes, vous pouvez réduire cette valeur à 1 heure (voire moins selon vos besoins).

Vous pouvez également activer un mécanisme de notification automatique qui permet au serveur secondaire d'être averti immédiatement de tout changement. À réception de ce signal, le serveur secondaire déclenchera alors un transfert de zone. Il suffit pour cela d'ajouter, dans l'onglet " Notification ", les adresses IP des serveurs secondaires.

LA BASE DE DONNÉES DU DNS

La base de données consiste en des fichiers ASCII contenant des **enregistrements** appelés **RR** (*Resource Record*) dont le format générique est le suivant :

nom [ttl] [IN] RR paramètres

nom Désigne le nom du domaine. S'il est omis, c'est le même que celui du SOA.

ttl Time To Live. Indique pendant combien de secondes le *resolver,* qui aura fait une requête, pourra conserver cet enregistrement dans son cache. Le TTL est défini au niveau du SOA (et donc pour tous les RR situés dedans), mais peut, optionnellement, être défini pour chaque RR. Le délai de validité du cache est le maximum des valeurs *ttl* et *minimum*.

IN Désigne la classe d'adresse, dans notre cas l'Internet (on trouve aussi CH pour les adresses Chaos).

RR Nom de la ressource (SOA, NS, A, LNAME, NX, PTR, HINFO, etc.).

nom [ttl] [IN] **SOA** name e-mail serial refresh retry expire minimum

(*Start Of Authority*). Indique le nom de la zone pour laquelle le serveur a autorité (secondaire ou primaire), ainsi que les paramètres de mise à jour de la base de données.

name Désigne le serveur primaire de la zone.

e-mail Désigne l'adresse e-mail de la personne responsable de la zone.

serial Désigne le numéro de version du SOA.

refresh Indique le nombre de secondes au bout duquel le serveur secondaire doit redemander le SOA au serveur primaire.

retry Indique le nombre de secondes qui s'écoule entre deux tentatives de téléchargement du SOA par le serveur secondaire.

expire Indique le nombre de secondes au bout duquel le SOA ne sera plus valable après le délai indiqué par *refresh*. Au-delà de ce délai, le serveur secondaire ne doit plus répondre aux requêtes concernant ce SOA.

minimum Indique la valeur minimale du TTL des RR de cette zone.

• • •

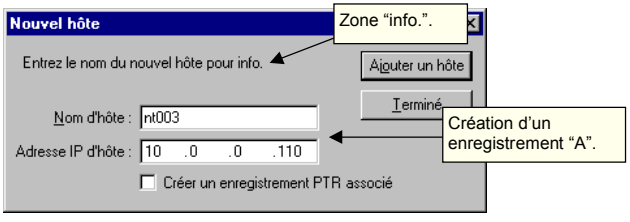
LA BASE DE DONNÉES DU DNS (SUITE)

[nom] [ttl] (*Name Server*)	IN	**NS**	nom_du serveur_DNS Indique le serveur (primaire ou secondaire) qui a autorité sur la zone.
[nom] [ttl] (*Address*)	IN	**A**	adresse_IP Indique l'adresse IP qui correspond au nom (serveur, routeur, etc.) demandé dans une requête.
alias [ttl] (*Canonical Name*)	IN	**CNAME**	nom_principal_de_l'objet Indique l'alias d'un objet.
nom [ttl] (*Mail eXchanger*)	IN	**MX**	priorité nom_du_MTA Indique le nom du MTA acheminant les messages à destination du domaine. 65535 = priorité basse, 1 = priorité haute.
inverse [ttl] (Pointer) **inverse**	IN	**PTR**	nom_machine Indique le nom qui correspond à l'adresse IP demandée dans une requête. Désigne l'adresse IP inverse, suivie de in-addr.arpa.
[nom] [ttl] (*Host Information*)	IN	**HINFO**	matériel système Champ d'information concernant l'objet (type de machine et d'OS).
[nom] [ttl]	IN	**AAAA**	adresse_IPv6 Indique l'adresse IPv6 qui correspond au nom demandé dans une requête (RFC 1886).

Les noms de serveurs indiqués dans les RR ne doivent pas être des alias.
Il existe d'autres enregistrements peu ou pas utilisés ou encore à l'état expérimental : WKS, TXT (RFC 1035), AFSDB, RP, X25, ISDN, RT (RFC 1183), NSAP (RFC 1706), GPOS (RFC 1712), SRV (RFC 2052) et KX (RFC 2230).

Activer la résolution de nom

Généralement, l'administrateur commence par remplir la base de données d'enregistrements " **A** ". Ce type d'enregistrement permet aux utilisateurs d'obtenir l'adresse IP correspondant au nom, qui leur est plus familier. C'est toute l'utilité du DNS.



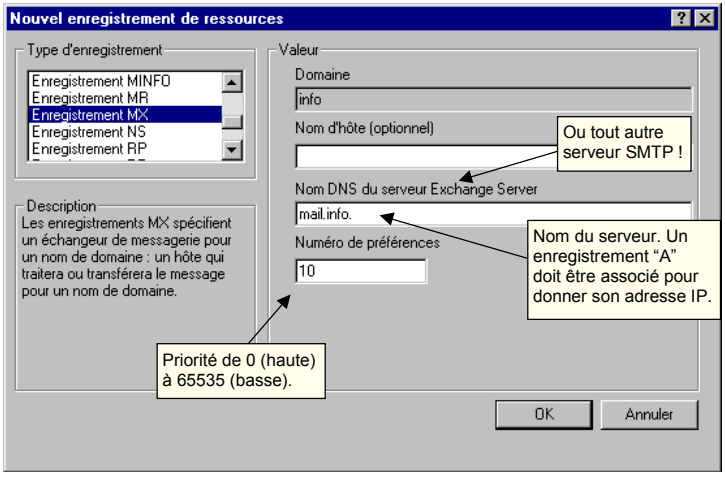
Cela a pour effet de créer l'enregistrement suivant :

```
nt003   IN      A       10.0.0.110
```

Désormais, le serveur DNS enverra au client l'adresse IP indiquée ci-dessus, à toute requête concernant ce nom.

Activer le routage de la messagerie

Un autre grand utilisateur du DNS est la messagerie SMTP (voir chapitre 3). Chaque MTA (*Message Transfer Agent*) s'appuie en effet sur les enregistrements " **MX** " pour router les messages vers le prochain MTA.



En définitive, deux enregistrements doivent être créés :

```
info.   IN      MX      10      mail.info.
@       IN      MX      10      mail
mail    IN      A       10.0.0.100
```

Ces deux notations sont équivalentes.

Ainsi, tous les messages à destination de xxx@info seront routés vers le serveur " mail " situé dans le domaine " info ".

Avec le mécanisme des priorités, il est possible de définir des serveurs de secours au cas où le MTA principal serait surchargé ou en panne. Il suffit pour cela de créer un autre enregistrement " MX " de priorité plus basse que celui créé précédemment :

```
info.   IN      MX      20      mail2.info.
mail2   IN      A       10.0.0.101
```

Enfin, il est également possible de définir un serveur " poubelle " recueillant tous les messages à destination de domaines inconnus :

```
*       IN      MX      100     mail9
```

Du bon usage des alias

L'utilisation d'un alias permet de dissocier la fonction (web, messagerie) de la nature des serveurs (nt001, unix002) ou de leur localisation dans un domaine ou un autre :

```
www    IN     CNAME  nt003.info.
pluton IN     CNAME  ux001.paris.compta.
```

Grâce à l'utilisation des alias, le changement des noms pluton et www suite à un déménagement sera plus facile à opérer que celui de nt003 qui est référencé par des enregistrements " A ".

Par exemple, on doit déplacer l'application intranet sur une nouvelle machine plus puissante. Il suffit de modifier le CNAME comme suit :

```
www    IN     CNAME  nt004.toulouse.info.
```

Configurer un serveur racine

Les serveurs racines ont tout simplement autorité pour la zone '**.**', c'est-à-dire sur l'ensemble de l'arbre DNS. Leur rôle est d'indiquer aux serveurs ne pouvant répondre aux requêtes de leurs clients, l'adresse du serveur pouvant les aider.

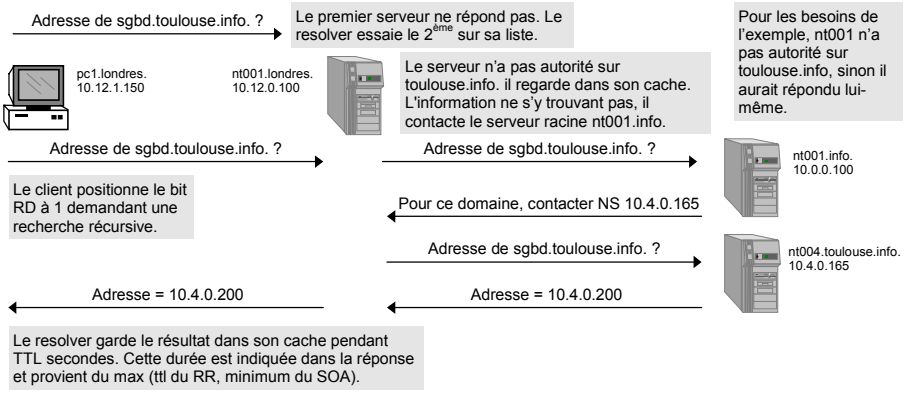
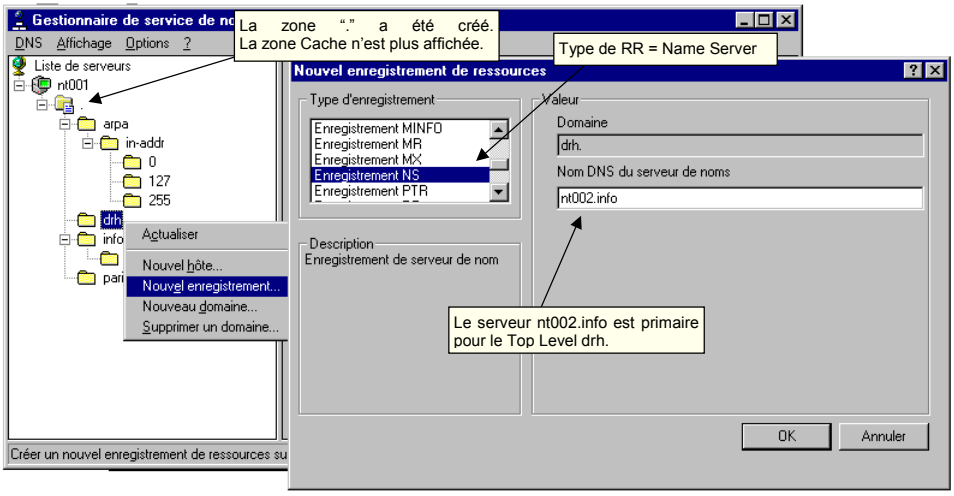


Figure 17-3. *Recherche DNS récursive.*

La recherche peut également être effectuée de manière itérative. Dans ce cas, le serveur DNS indique au client le nom du serveur DNS qui peut l'aider, et il revient au client d'effectuer lui-même la recherche.

Dans notre cas, nous commençons par déclarer un serveur primaire pour la zone " **.** " (ne pas choisir le nom de fichier " . ", mais, par exemple, le nom " racine.dns "). Puis, nous déclarons les serveurs primaires des domaines Top Level.



Cela produit le fichier suivant :

```
.       IN      SOA     nt001.info.  jlm.nt001.info. (
                2       ; serial : 2ème version
                1800    ; refresh : toutes les 30 min.
                300     ; retry : toutes les 5 minutes
                604800  ; expire : 48 heures après
                86400)  ; minimum : 24h dans le cache
                NS      nt001.info
                NS      nt004.toulouse.info

nt001.info              A       10.0.0.100
nt004.toulouse.info     A       10.4.0.165

paris                   NS      nt001.info
info                    NS      nt001.info
drh                     NS      nt002.info

nt002.info.             A       10.0.0.124
```

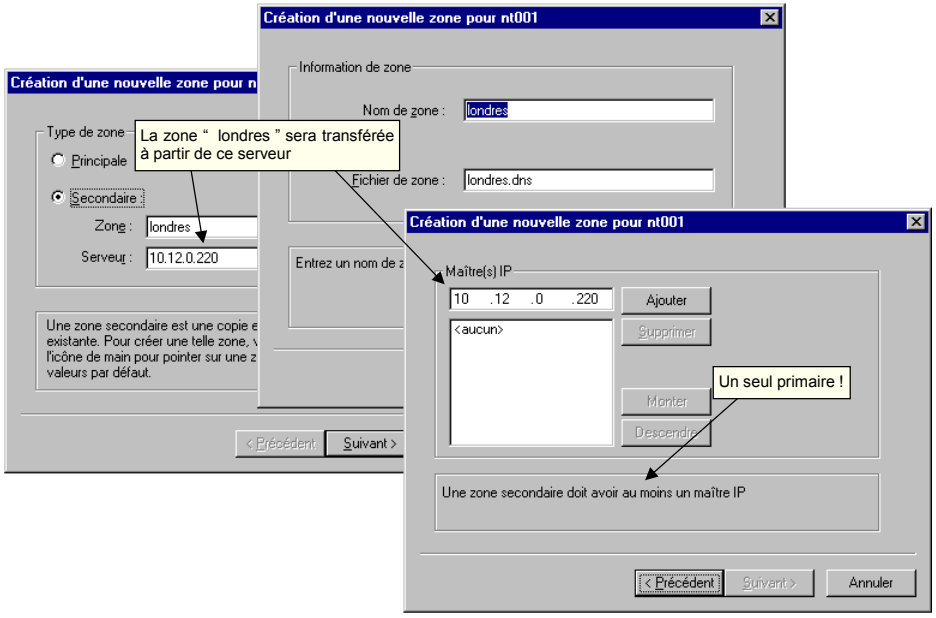
Liste des serveurs ayant autorité sur la racine.

Liste des serveurs ayant autorité sur les Top Level paris, info et drh.

Configurer un serveur secondaire

Un serveur secondaire pour une zone est un serveur qui a autorité sur ladite zone, mais qui ne peut pas modifier la base de données correspondante. Pour cela, il demande auprès du serveur primaire **le transfert de la zone**, ce qui lui permet ensuite de répondre aux requêtes de la même manière qu'un serveur primaire.

Sur ce type de serveur, une zone est déclarée secondaire en indiquant l'adresse IP du serveur primaire à partir duquel transférer la zone.



Il est à noter que le volume de données représenté par un transfert de zone est peu important, d'autant plus si les serveurs supportent une mise à jour incrémentale (RFC 1995).

Configurer un serveur cache

Tous les serveurs DNS conservent en mémoire cache les réponses des requêtes précédentes. Le serveur cache joue le même rôle, mais présente la particularité de n'avoir aucune autorité sur une quelconque zone : le serveur n'est ni primaire ni secondaire.

La configuration d'un serveur cache se résume donc à renseigner uniquement le fichier " cache.dns " qui liste les serveurs racines.

La durée de validité des enregistrements dans le cache est déterminée par le maximum des deux valeurs suivantes : le paramètre " *minimum TTL* " du SOA et le TTL de chaque enregistrement si celui-ci est spécifié.

Déléguer l'autorité à un autre serveur

Pour des questions d'organisation, il est maintenant opportun de déléguer la gestion de la zone " toulouse.info " aux exploitants de ce site. Pour cela, la procédure est la suivante :

1. Configurer le serveur de Toulouse en secondaire de " toulouse.info ", afin de transférer cette zone.
2. Configurer ensuite le serveur de Paris en secondaire pour la zone " toulouse.info ".
3. Basculer enfin le serveur de Toulouse en primaire pour la zone " toulouse.info ".
4. Modifier les enregistrements NS sur les différents serveurs concernés, de manière à pointer sur le nouveau serveur primaire.
5. Si l'ancien serveur primaire ne doit pas faire office de serveur secondaire du domaine " toulouse.info ", supprimer toute référence à cette zone.

Sous le gestionnaire DNS de Windows, il faut, en plus, créer un domaine " toulouse.info ", de manière à extraire les données du fichier " info.dns " dans un autre fichier, " toulouse.info.dns ", par exemple.

Dans le serveur primaire de " info ", la zone déléguée apparaîtra alors comme suit :

```
;
;  Delegated sub-zone:  toulouse.info.
;
toulouse              NS    nt001
;  End delegation
```

Les domaines de résolution inverse

Un domaine spécifique, appelé domaine de résolution inverse et noté **in-addr.arpa**, est utilisé pour trouver un nom à partir d'une adresse IP. Un domaine correspondant au réseau 10.4.0.0 sera ainsi noté 4.10.in-addr.arpa. (notation inverse de l'adresse IP).

Les domaines de résolution inverse se manipulent de manière identique aux domaines de noms. Chacun des 4 nombres de l'adresse IP est considéré comme étant un domaine qui peut être délégué. Un serveur peut ainsi être primaire pour le domaine 10.in-addr.arpa, et déléguer son autorité pour 15.10.in-addr.arpa.

La résolution inverse permet :

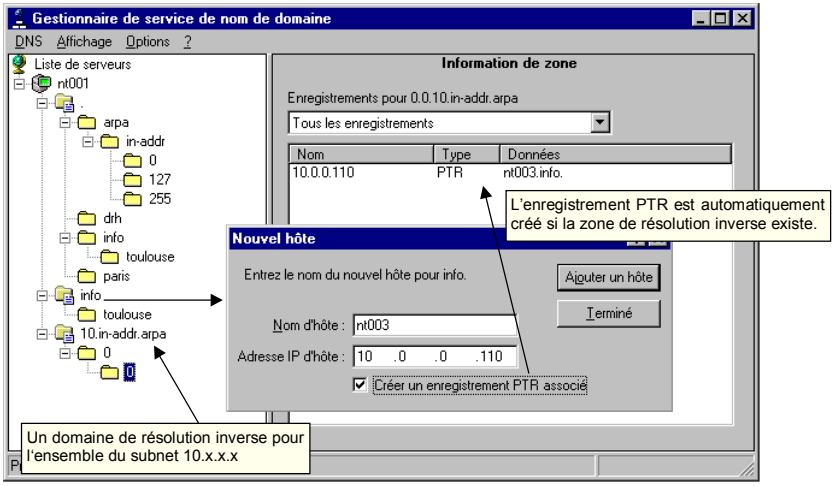
- De découvrir les routeurs d'un sous-réseau IP. Le client reçoit le nom des routeurs et peut ensuite lancer une requête pour en connaître les adresses IP. Pour des questions de sécurité, il est donc déconseillé d'utiliser cette facilité.
- À un serveur de s'assurer qu'un client qui se présente avec une adresse IP appartient bien à un domaine autorisé et/ou est bien celui qu'il prétend être. Certains serveurs FTP de l'Internet nécessitent que les clients soient référencés dans la base DNS sous forme d'enregistrement PTR.

- De référencer les noms de réseaux permettant à une station d'administration d'afficher les noms au lieu des adresses IP.
- Au programme **nslookup** (voir plus loin) de fonctionner correctement. En effet, le serveur à partir duquel la commande est lancée doit être référencé.

Une arborescence similaire doit donc être créée. Et, là encore, le DNS permet toutes sortes de fantaisies.

Par exemple, il n'y a pas obligatoirement de correspondance entre domaines de noms et domaines de résolution inverse. Les serveurs primaires pour un réseau peuvent ainsi ne pas l'être pour les domaines qui le contiennent. La création automatique de PTR est alors rendue difficile.

Il est donc conseillé de limiter le nombre de ce type de zones à une par subnet IP principal, le réseau 10 dans notre cas.



Le fichier d'initialisation

Le serveur DNS de Microsoft peut fonctionner sans l'interface graphique, à la manière des premiers serveurs DNS sous Unix. Le système fonctionne alors uniquement à partir des fichiers ASCII situés dans le répertoire \Winnt\System32\Dns.

Pour passer en mode texte, il faut supprimer la variable *EnableRegistryBoot* de la base des registres Windows au niveau de la clé " HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Services\Dns\ Parameters ".

Un nouveau fichier doit alors être renseigné : il s'agit du fichier d'initialisation du DNS tel qu'utilisé sous Unix, appelé **boot** :

```
;
; Fichier Boot de nt001.info
;
cache          .                cache.dns
primary        info             info.dns
secondary      toulouse.info 10.4.0.165      toulouse.info.dns
primary        10.in-addr.arpa        10.in-addr.arpa.dns
```

Nom du fichier cache indiquant les serveurs racines.

Adresse IP du serveur primaire

Précise les zones et noms des fichiers de chaque SOA pour lequel le serveur est primaire ou secondaire.

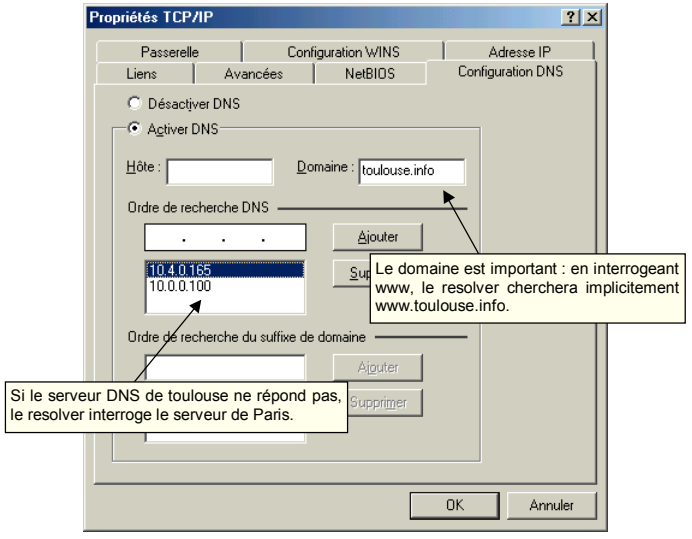
Configurer les clients DNS

Dans la terminologie DNS, un client est appelé **resolver**. Ce petit morceau de programme est directement sollicité par toutes les applications fonctionnant en réseau, telles que le navigateur web. Il se contente d'interroger des serveurs DNS.

Sa configuration consiste simplement à indiquer le domaine dans lequel il se trouve, ainsi que la liste des adresses IP des serveurs DNS susceptibles de répondre à ses requêtes.

Une fois de plus, le DNS offre beaucoup de souplesse :

- le client interroge le premier serveur de la liste puis, s'il ne répond pas, le second et ainsi de suite ;
- les serveurs peuvent être de type cache, primaire ou secondaire ;
- le client peut être situé dans un domaine différent des serveurs qu'il interroge.

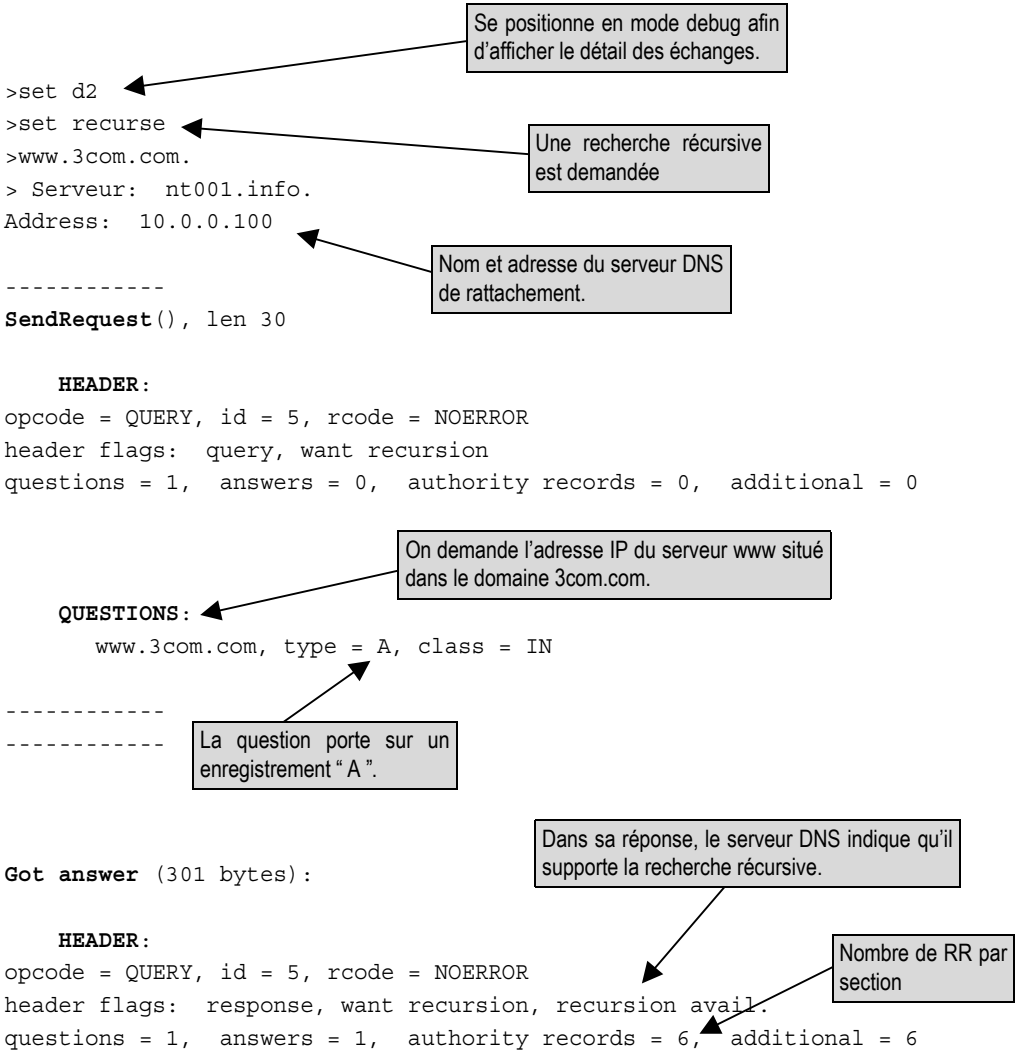


L'utilisateur peut formuler une demande sur un **nom complet**, tel que " www.info. " (un nom terminé par un point). Aucun suffixe ne sera alors ajouté.

S'il lance une recherche sur un **nom relatif**, par exemple www (un nom qui n'est pas terminé par un point), le resolver le recherchera par défaut dans le même domaine que celui configuré. S'il reçoit une réponse négative, il ajoutera le suffixe " .info ", puis un autre suffixe en fonction de la configuration.

Vérifier le fonctionnement du DNS

L'utilitaire de base pour tout administrateur DNS est le **nslookup** qui s'exécute à partir d'une fenêtre DOS de Windows NT :



```
    QUESTIONS:
       www.3com.com, type = A, class = IN
    ANSWERS:
    ->  www.3com.com
       type = A, class = IN, dlen = 4
       ttl = 3645 (1 hour 45 secs)
    AUTHORITY RECORDS:
    ->  3COM.COM
       type = NS, class = IN, dlen = 9
       nameserver = FOUR11.3COM.COM
       ttl = 38819 (10 hours 46 mins 59 secs)
...... suivent 5 autres RR ......
    ADDITIONAL RECORDS:
    ->  FOUR11.3COM.COM
       type = A, class = IN, dlen = 4
       internet address = 129.213.128.98
       ttl = 92825 (1 day 1 hour 47 mins 5 secs)
...... suivent 5 autres RR ......
```

La réponse est structurée en 4 sections : question, réponse, enregistrements NS et les autres enregistrements.

Par défaut, l'enregistrement " A " est demandé, mais il est possible de demander d'autres types d'enregistrements, tels que le " SOA " :

```
>set d2
>set recurse
>set querytype=soa
>www.3com.com.
> Serveur:  ns1.club-internet.fr
Address:  194.117.200.10


------------
SendRequest(), len 26
    HEADER:
opcode = QUERY, id = 5, rcode = NOERROR
header flags:  query, want recursion
questions = 1,  answers = 0,  authority records = 0,  additional = 0

    QUESTIONS:
       3com.com, type = SOA, class = IN
------------
------------
```

```
Got answer (320 bytes):

    HEADER:
opcode = QUERY, id = 5, rcode = NOERROR
header flags:  response, want recursion, recursion avail.
questions = 1,  answers = 1,  authority records = 6,  additional = 6

    QUESTIONS:
       3com.com, type = SOA, class = IN
    ANSWERS:
    ->  3com.com
       type = SOA, class = IN, dlen = 42
       ttl = 68436 (19 hours 36 secs)
       primary name server = four11.3com.com
       responsible mail addr = hostmaster.3com.com
       serial  = 1998090100
       refresh = 10800 (3 hours)
       retry   = 3600 (1 hour)
       expire  = 604800 (7 days)
       default TTL = 10800 (3 hours)
    AUTHORITY RECORDS:
    ->  3com.com
       type = NS, class = IN, dlen = 2
       nameserver = four11.3com.com
       ttl = 38922 (10 hours 48 mins 42 secs)
...... etc. ......
```

On retrouve les paramètres du SOA tels que l'administrateur de 3com les a définis.

Annexes