

## Réseaux : DNS4

1. Présentation théorique .....	1
1. Introduction. ....	1
1. Structure du DNS .....	2
2. Le serveur de noms. ....	2
3. Résolution des noms.....	3
4. Les fichiers DNS .....	4
4.1. Le fichier d'associations directes (Forward Mapping File).....	4
4.2. Le fichier d'associations inverses. ....	6
5. Le fichier de cache. ....	7
6. Le fichier de BOOT.....	8
7. Exemple complet des fichiers de zone. ....	10
2. Serveur DNS sur NT serveur 4.0 .....	11
1. Installation du service DNS.....	11
1.1. Vérification des informations DNS sous Windows NT.....	11
1.2. Installation du service DNS Microsoft.....	12
2. Configuration des domaines et des zones. ....	13

[Les modifications que j'ai apportées : notes de cours]

### 1. Présentation théorique

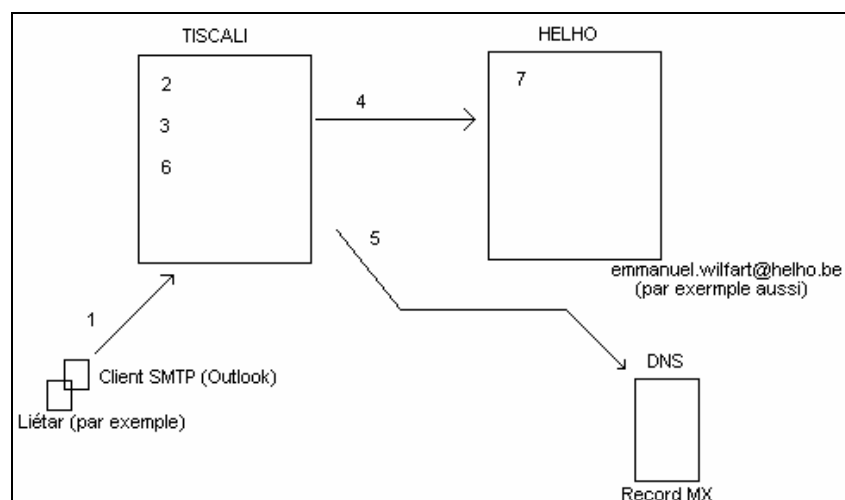
#### 1. Introduction.

TCP/IP utilise des adresses codées sur 32 bits ( 4x8 bits) pour acheminer un datagramme vers une destination.  
Exemple: **193.191.131.2**.

DNS qui est l'abréviation de Domain Name System est un ensemble de protocoles et services qui permet aux utilisateurs d'un réseau d'utiliser un nom symbolique hiérarchisé pour un ordinateur au lieu d'avoir à retenir et à utiliser les adresses IP. Ce système est utilisé de façon intensive sur Internet et dans certains réseaux locaux privés.

[Reverse DNS : permet de voir si le nom de domaine associé dans le datagramme correspond à l'IP annoncé.

Mécanismes de 2 serveurs SMTP :



0. La machine va voir dans le fichier host, puis dans la cache.
1. Le client prend contact avec le serveur SMTP de Tiscali.
2. Le serveur SMTP accepte la demande ; pour l'utilisateur, le mail est envoyé.
3. Le serveur récupère l'adresse de destination.
4. Le serveur rentre en contact avec le serveur SMTP de Helho.

5. Le serveur de Tiscali envoie une requête sur le serveur DNS et demande qui est le serveur SMTP de Helho. Le serveur de Tiscali connaît le nom de domaine de Helho.

6. Quand il récupère l'adresse, il envoie le paquet.

7. Le serveur SMTP de Helho peut accepter ou pas le paquet. Si Helho n'accepte pas, Tiscali enverra un message d'erreur. Si Helho ne répond pas, le paquet est placé en queue.]

La fonction la plus connue du DNS est de faire correspondre un nom symbolique et une adresse IP. Par exemple, pour le site WEB de la Haute Ecole, l'adresse IP est **193.191.131.2**. Il est plus aisé pour les internautes de se rappeler du nom [www.helho.be](http://www.helho.be) au lieu de cette adresse IP. De plus, alors que le nom symbolique peut rester le même, il est possible pour l'administrateur réseau de changer s'il le désire l'adresse IP associée à ce nom.

Avant l'implémentation de DNS, l'utilisation des noms symboliques se faisait par l'usage de fichiers HOSTS qui contenait une liste des adresses IP et des noms associés. Sur Internet, ce fichier était administré de façon centrale et l'on devait périodiquement charger une copie de ces fichiers. Comme le nombre de machines sur Internet n'a fait que grandir, cette solution n'a rapidement plus été viable. La meilleure solution devint donc DNS.

DNS se situe au niveau de la couche 7 du modèle OSI et peut donc utiliser indifféremment UDP ou TCP comme protocole de liaison.

## 1. Structure du DNS

Le service des noms de domaines (DNS), comme son nom l'indique, travaille en divisant l'espace de travail Internet en un ensemble de domaines ou réseaux qui peuvent être à leur tour divisés en sous domaines.

Cette structure ressemble à une arborescence dont le sommet est appelé le niveau supérieur du domaine (top level domaine). Ce niveau est géré par l'Internet Network Information center mieux connu par son abréviation Internic. Il comprend des domaines pour les organisations et un domaine par pays. Ces domaines sont identifiés par un groupe de deux à trois lettres conformément au standard international 3166.

Nom de domaine	Type d'organisation
COM	Pour les sociétés commerciales
EDU	Pour les organisations éducationnelles
GOV	Pour les gouvernements
MIL	Pour les organisations militaires
NET	Pour les réseaux
ORG	Pour les organisations non gouvernementales
INT ...	Pour les organisations internationales

Pour les pays, on retrouve par exemple be pour la Belgique, fr pour la France, uk pour le royaume uni...

Un domaine peut contenir soit des hôtes (host) ou des sous domaines. Chaque domaine s'identifie dans l'arborescence par rapport à son parent en étant séparé par un point (dot). On parlera souvent pour les noms de domaines de noms pointés. Le site de la Haute Ecole est un sous domaine du domaine be et de ce fait, notre domaine s'identifie dans l'arborescence par le nom **helho.be**. Chaque sous domaine peut à son tour contenir un sous domaine ou des hôtes (host). On pourra donc retrouver des ordinateurs tels que [www.helho.be](http://www.helho.be) ou alors info3.helho.be, sous domaine comprenant l'ordinateur [www.info3.helho.be](http://www.info3.helho.be).

Dans un domaine local, un ordinateur peut être authentifié par un nom relatif lorsque le serveur de noms connaît la destination dans l'arborescence et qu'il n'a donc pas besoin d'acheminer le datagramme sur le réseau internet ou lorsque le serveur de noms connaît le nom relatif et qu'il peut donc directement l'acheminer.

Si la destination se trouve sur le réseau Internet, l'usage du nom absolu est nécessaire.

Exemple:

- En interne, on peut directement accéder à l'ordinateur baby par son nom relatif: <http://baby>.
- Par l'Internet, l'accès à cet ordinateur doit se faire par son nom absolu: <http://baby.helho.be>.

## 2. Le serveur de noms.

Chaque serveur de noms de domaine gère une zone distincte du réseau. L'ensemble des machines gérées par le serveur de noms est appelé une zone. Plusieurs zones peuvent être gérées par un seul serveur de noms.

On peut imaginer le domaine helho.be comprenant la zone helho.be et la zone info3.helho.be. Ces deux zones peuvent être gérées par un serveur de noms unique ou par deux serveurs distincts. Ces serveurs sont dits avoir l'autorité sur leur zone.

La plupart des zones possèdent plusieurs serveurs de noms:

- Un serveur de noms primaire
- Un serveur de nom secondaire ou de sauvegarde.

Un serveur de noms primaire est un serveur qui reçoit les données pour sa zone de fichiers locaux. Tout changement dans une zone tels que l'ajout de domaines ou d'hôtes se fait sur le serveur de noms primaire.

Un serveur de noms secondaire reçoit ses données pour sa zone d'un autre serveur de noms qui a autorité pour cette zone. Ces serveurs communiquent à travers le réseau par un protocole de transfert de zone sous TCP.

DNS apparaît comme un ensemble de zones emboîtées. Chaque serveur de noms communique avec un autre serveur de noms juste au dessus de lui et éventuellement juste en dessous de lui si il y en a un. Chaque zone a au moins un serveur de noms responsable de connaître la correspondance entre les noms des ordinateurs et les adresses dans sa zone. Chaque serveur connaît aussi l'adresse d'au moins un autre serveur de noms du Top Level Domain. Les messages qui transitent entre les serveurs de noms utilisent le protocole UDP (User Datagram Protocol) du fait qu'une méthode sans connexion apporte de meilleures performances. Cependant TCP est utilisé pour la mise à jour des bases de données du fait de sa fiabilité accrue.

[Différence zone-domaine : le domaine est géré par un seul serveur et un serveur est capable de gérer plusieurs zones.]

Quand une application d'utilisateur a besoin de résoudre un nom symbolique en une adresse réseau, une demande est envoyée vers un service de résolution. Ce dernier envoie la demande vers un serveur de nom qui va déterminer dans ses tables s'il peut fournir l'adresse correspondante. Si le serveur ne peut fournir cette adresse, il peut envoyer la demande vers un autre serveur de noms. A la fois les serveurs de noms et les résolveurs utilisent une cache locale permettant de mémoriser le résultat des requêtes les plus récentes à l'extérieur de la zone.

### 3. Résolution des noms.

Il y a deux types de demandes qu'un client peut faire à un serveur DNS: récursif, itératif et inverse. Quand on parle de résolution de noms, il faut garder à l'esprit qu'un serveur DNS peut être le client d'un autre serveur DNS.

- Demandes récursives:

Dans une demande récursive, le serveur de noms auquel la requête est envoyée doit répondre avec la donnée demandée ou avec une erreur pour renseigner que la donnée du type demandée n'existe pas ou que le nom de domaine spécifié n'existe pas. Ce type de demande est typiquement celle envoyée par un client (resolver) vers un serveur DNS.

- Demandes itératives:

Dans une demande itérative, le serveur de nom auquel la requête est envoyée doit donner une réponse complète en retour à la demande. C'est une demande typique faite par un serveur DNS à un autre serveur DNS qui a reçu une demande récursive.

Supposons qu'un étudiant veuille par son navigateur accéder au site [www.yahoo.com](http://www.yahoo.com) à partir d'un des ordinateurs du laboratoire d'informatique. Le navigateur, via son resolver, envoie une demande récursive vers le serveur de noms du laboratoire (193.191.131.2). Celui ci doit envoyer plusieurs demandes itératives:

- a) Demande envoyée vers le serveur qui a autorité pour la zone .com. Celui ci envoie en retour l'adresse du serveur de noms qui a autorité pour la zone yahoo.
- b) Demande envoyée vers le serveur qui a autorité pour la zone yahoo.com. Celui ci envoie en retour l'adresse de l'hôte www.

Le serveur de noms du laboratoire peut donc maintenant envoyer l'adresse IP correspondant au nom symbolique [www.yahoo.com](http://www.yahoo.com).

## 4. Les fichiers DNS

30 sept. 04

### 4.1. Le fichier d'associations directes (Forward Mapping File)

Un fichier de zone est un fichier qui contient des enregistrements de ressource (ressource records) pour le partie du domaine pour laquelle la zone est responsable. Ce fichier est dans un format ASCII et de ce fait peut être facilement mis à jour.

[Intérêt : marche grand pas d'interface graphique]

Fichier d'associations directes prend en charge les demandes de résolution directe

Fichier texte dans lesquels on retrouve des enregistrements (telle machine a telle adresse IP)

1<sup>er</sup> enregistrement SOA (Start Of Authority)

Le premier enregistrement dans n'importe quel fichier de zone est l'enregistrement SOA sous la forme suivante:

IN SOA <hôte source> <adresse email de contact><numéro de série><**temps de rafraîchissement**><**intervalle d'essai**><**temps d'expiration**><TTL>

En **gras**, les items qui sont en rapport avec le serveur DNS de sauvegarde.

- hôte source: l'hôte sur lequel le fichier est maintenu
- Adresse email de contact: l'adresse email Internet pour la personne responsable pour le fichier de zone pour le domaine. [Au niveau de l'enregistrement, l'adresse email s'écrit avec un point qui remplace le @.]
- Numéro de série: le numéro de version du fichier de zone. Ce numéro est incrémenté à chaque fois que le fichier est modifié. Si on oublie, le serveur DNS de sauvegarde ne fera pas de m à j.
- Temps de rafraîchissement: l'écart de temps en seconde qu'un serveur de nom secondaire doit attendre entre deux vérifications auprès du serveur principal pour vérifier si le fichier de zone a été modifié et qu'un transfert de zone soit demandé.
- Temps d'essai: intervalle de temps en seconde pendant lequel un serveur secondaire doit attendre avant de réessayer un transfert de zone qui a raté.
- Temps d'expiration: intervalle de temps en seconde pendant lequel un serveur secondaire doit continuer à essayer de charger une zone. Après l'expiration de ce temps, les informations de la vieille zone seront écartées.
- TTL (time to live): intervalle de temps en seconde pendant lequel un serveur DNS est autorisé à caché les enregistrements de ressource de son fichier de zone.
- [Exemple → *hesit.be* (ou@) IN SOA ns.helho.be. root.helho.be. + les temps + TTL.

Le point à la fin de chaque nom d'enregistrement indique que le nom est complet.

En *italique*, facultatif.

@ pour remplacer le nom de la zone associée au fichier (raccourci !)

Vieux serveur Web(xxxx) →transfert→ Nouveau serveur Web (xxxxy)

Pour migrer : couper xxxx et remplacer le nom xxxxy par xxxx. Le TTL enverra encore des requêtes sur le vieux serveur. Donc, il y a mieux !

Laisser les deux serveurs et dire dans le serveur DNS que l'adresse [www.truc.be](http://www.truc.be) mpointe vers xxxy. Puis, on peut couper le xxxx après un certain temps.

Le SOA doit être le premier enregistrement !!!]

On peut retrouver ensuite les ressources suivantes:

<i>Numéro</i>	<i>Code</i>	<i>Description</i>
1	A	Network address
2	NS	Authoritative name server
3	MD	Mail destination; now replaced by MX
4	MF	Mail forwarder; now replaced by MX
5	CNAME	Canonical alias name → dire ce nom est identique à un autre
6	SOA	Start of zone authority
7	MB	Mailbox domain name
8	MG	Mailbox member
9	MR	Mail rename domain
10	NULL	Null resource record

11	WKS	Well-known service
12	PTR	Pointer to a domain name
13	HINFO	Host information
14	MINFO	Mailbox information
15	MX	Mail exchange
16	TXT	Text strings
17	RP	Responsible person
18	AFSDB	AFS-type services
19	X.25	X.25 address
20	ISDN	ISDN address
21	RT	Route through

Dans cette table, certains enregistrements sont obsolètes (3 et 4) et d'autres considérés comme expérimentaux (13 et 17-21).

#### ***L'enregistrement d'adresse:***

Un enregistrement d'adresse est utilisé pour associer de façon statique un nom d'hôte et une adresse IP dans une zone. Il y a autant d'entrées que d'hôtes qui nécessitent une association statique incluant les stations de travail, les serveurs de noms, les serveurs de messagerie...

Syntaxe:            <nom d'hôte>    IN A    <adresse IP de l'hôte>

Un exemple d'enregistrement d'adresse:

```

baby    IN A    193.191.131.3
mail    IN A    193.191.131.2

```

#### ***L'enregistrement du serveur de nom ayant autorité:***

L'enregistrement du serveur de nom pointe sur le nom de serveur qui a autorité pour une zone particulière.

Syntaxe:            <domaine>            IN NS    <nom du serveur>

Un exemple d'enregistrement de serveur de nom:

Soit le domaine helho.be. On peut imaginer un sous domaine info3.helho.be dont l'entrée correspondante dans le fichier de zone du domaine helho serait:

```

info3.helho.be.            IN NS    ns.info3.helho.be.

```

ns.info3.helho.be sera donc le serveur de nom ayant autorité pour la zone info3.helho.be

#### ***L'enregistrement d'échange de messagerie électronique:***

Cet enregistrement permet de renseigner l'hôte qui gère la messagerie pour ce domaine. Si plusieurs enregistrements existent, le resolver essaiera de contacter le serveur de messagerie par ordre de préférence, partant de la valeur la plus basse jusqu'à la valeur la plus élevée.

Syntaxe:            <domaine>            IN MX    <preference><nom du serveur de messagerie>

Un exemple d'enregistrement de serveur de messagerie:

```

helho.be      IN MX 1      mail.helho.be
helho.be      IN MX 2      student.helho.be

```

Un courrier adressé à [bil@helho.be](mailto:bil@helho.be) sera dans un premier temps délivré à [bil@mail.helho.be](mailto:bil@mail.helho.be) et si la boîte n'existe pas sur ce serveur, il sera dans un deuxième temps transmis à [bil@student.helho.be](mailto:bil@student.helho.be). [bil@helho.be se trouve-t-il sur mail.helho.be ou student.helho.be ? Il ne peut se trouver sur les deux. On met une préférence.]

#### *L'enregistrement du nom canonique:*

Cet enregistrement est également appelé alias mais est techniquement référencé comme l'entrée Canonical Name (CNAME). Ces enregistrements permettent l'utilisation de plus d'un nom pour un hôte unique. [Utile pour un serveur qui héberge plusieurs sites.]

Syntaxe: <nom d'alias de l'hôte> IN CNAME <nom de l'hôte>

Un exemple d'enregistrement de nom canonique:

```

ns      IN A      193.191.131.2
www     IN CNAME ns
FTP     IN CNAME ns

```

#### *L'enregistrement du service bien connu:*

Cet enregistrement contient trois champs décrivant les services supportés à l'adresse spécifiée par l'enregistrement.

Syntaxe: <Nom de domaine complet> IN WKS <adresse>  
< liste des protocoles supportés>

#### *4.2. Le fichier d'associations inverses.*

La fonction principale d'un serveur DNS est de pouvoir retrouver l'adresse IP d'un hôte à partir de son nom symbolique. Pourtant, du fait que certaines applications utilisent comme sécurité le fait de pouvoir retrouver un nom de domaine sur base de l'adresse, en vue de limiter l'accès à certains services uniquement aux membres d'un domaines, un domaine spécial "in-addr.arpa" a été créé dans l'espace de nom DNS. Les nœuds dans le domaine in-addr.arpa sont nommés après le numéro de l'adresse IP dans une représentation octet pointé. L'adresse IP pointé contient des parties dont l'importance croît de la gauche vers la droite mais que le nom de domaine contient des parties dont l'importance décroît de la gauche vers la droite, l'ordre des octets de l'adresse IP doit être inversé quand on construit l'arborescence DNS in-addr.arpa.

In-addr.arpa utilise un enregistrement PTR pour pointer de l'adresse vers le nom.

Syntaxe: <adresse IP> IN PTR <nom de l'hôte>

Exemple d'enregistrement:

```

2.131.191.193.IN-ADDR.ARPA. PTR www.helho.be
3.131.191.193.IN-ADDR.ARPA. PTR baby.helho.be

```

Pour adresse de classe B, on pourrait retrouver l'enregistrement suivant:

55.157.in-addr.arpa

Ces enregistrements sont placés dans le fichier IN-ADDR-ARPA pour en faciliter l'usage.

Exemple : on possède un réseau 193.191.131.0, masque de sous-réseau 255.255.255.0  
Si on veut prendre en charge la résolution inverse, nous devons ajouter les lignes suivantes :

Fichier **131.191.193.IN-ADDR.ARPA**

Adresse IP inversée du réseau

```

IN SOA
IN NS      → ces enregistrements dans cet ordre
IN PTR
IN SOA     2      IN PTR      ns.helho.be

```

Adresse IP 193.191.131.2

[Domaine HELHO : 193.191.131.0 à 193.191.131.31 avec un masque 255.255.255.224

Or c'est Belnet qui est contacté en 1er lors d'une demande de résolution inverse, Belnet utilise la délégation de zone pour les adresses IP attribuées à la HELHO pour dire : pour les adresses 193.191.131.0 à 193.191.131.31, c'est la HELHO qui s'en occupe. (Belnet donne alors un nom de fichier spécifique à utiliser pour l.]

## 5. Le fichier de cache.

Le fichier de cache contient les informations nécessaires pour résoudre les noms à l'extérieur du domaine qui a autorité. Il contient les noms et adresses du serveur de nom racine. Ce fichier peut être chargé à l'adresse suivante: [FTP://rs.internic.net/domain/named.cache](ftp://rs.internic.net/domain/named.cache)

```

; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC registration services
; under anonymous FTP as
; file /domain/named.root
; on server FTP.RS.INTERNIC.NET
; -OR- under Gopher at RS.INTERNIC.NET
; under menu InterNIC Registration Services (NSI)
; submenu InterNIC Registration Archives
; file named.root
;
; last update: Aug 22, 1997
; related version of root zone: 1997082200
;
; 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
;
; formerly C.PSI.NET
;
. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
;
; formerly TERP.UMD.EDU
;
. 3600000 NS D.ROOT-SERVERS.NET.

```

```

D.ROOT-SERVERS.NET.      3600000      A      128.8.10.90
;
; formerly NS.NASA.GOV
;
.                          3600000      NS      E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A      192.203.230.10
;
; formerly NS.ISC.ORG
;
.                          3600000      NS      F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A      192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                          3600000      NS      G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A      192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                          3600000      NS      H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A      128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                          3600000      NS      I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A      192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.                          3600000      NS      J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A      198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.                          3600000      NS      K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A      193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.                          3600000      NS      L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A      198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                          3600000      NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A      202.12.27.33
; End of File

```

## 6. Le fichier de BOOT

Ce fichier est nommé `named.boot`. Les lignes dans ce fichier ont les significations suivantes:

### *Directory:*

C'est le chemin qui indique l'endroit où se trouvent l'ensemble des fichiers utilisés par le serveur DNS. Si le répertoire n'est pas renseigné, ce sera par défaut `/etc` qui sera choisi.

Exemple: `directory /etc/namedfiles`

### *Cache:*

Les informations situées dans la cache sont indispensables pour que le serveur DNS puisse fonctionner correctement.

### Primary:

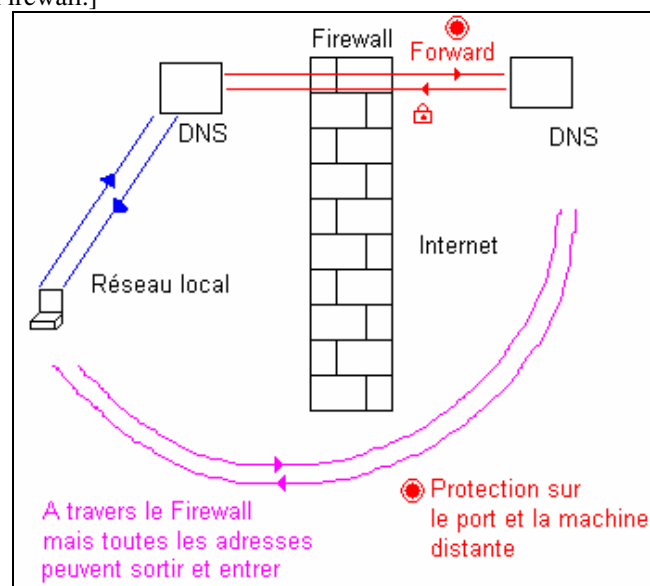
C'est un des domaines pour lequel la machine a autorité. Il faut y placer le nom du domaine complet. Vous ne devez pas oublier de gérer les recherches directes et inverses. La première valeur est le domaine à ajouter à chaque nom inclus dans ce fichier. Le nom à la fin de la ligne est le nom du fichier ( relatif au répertoire renseigné ou le répertoire par défaut /etc). Le nom du fichier peut inclure un caractère "slash" pour référencer un sous répertoire (utile si vous avez plusieurs domaines à gérer avec le souhait de placer l'ensemble des fichiers de chaque domaine dans un répertoire distinct).

```
Exemple:      primary      ecel.uwa.edu.au      ecel.uwa.domain
              primary      0.0.127.in-addr.arpa  0.0.127.domain
              primary      4.95.130.in-addr.arpa  4.95.130.domain
```

### Forwarders:

C'est une liste d'adresses IP pour le transfert des requêtes de sites vers le serveur de nom qui a autorité pour la zone au dessus de vous.

[Si le serveur reçoit une demande dans les adresses dont il a la charge, il s'en occupe. Si on veut atteindre Internet (donc des IP dont le serveur DNS local n'a pas la charge), le DNS local forwarde (transfère) les demandes vers le serveur DNS extérieur. Les réponses reviennent vers le serveur DNS local puis vers la machine. Au point de vue du firewall, seul le serveur DNS peut « sortir ». Les serveurs intranet peuvent être utilisés comme serveur de cache : ne sert à rien au niveau sécurité. Plus rapide grâce à la cache, car on ne repasse plus à travers le Firewall.]



### Secondary:

Une ligne "secondaire" indique que vous souhaitez être un serveur secondaire pour le domaine renseigné. Vous devez avoir un serveur DNS secondaire pour votre site mais vous n'êtes pas obligé d'être le serveur secondaire pour quelqu'un d'autre. Si vous voulez être serveur secondaire pour un autre domaine, il faut ajouter la ligne suivante:

```
secondary      gu.uwa.edu.au      130.95.100.3      sec/gu.uwa.edu.au
```

Cette ligne permet à votre serveur de nom de rentrer en contact avec les autres machines pour voir si des informations peuvent être obtenues sur ces domaines. Dès que la copie des noms est obtenue, votre serveur peut fournir toute information demandée dans ce domaine comme si votre serveur avait autorité pour ce domaine.

## 7. Exemple complet des fichiers de zone.

Exercices 1-2  
mondomaine.be

- ns.mondomaine.be (serveur ayant autorité sur mondomaine.be)
- 193.191.131.2

Serveur web	<a href="http://www.mondomaine.be">www.mondomaine.be</a>	193.191.131.10
Serveur pop3	pop3.mondomaine.be	193.191.131.11
Serveur SMTP	relay.mondomaine.be	193.191.131.12
Serveur FTP	<a href="http://ftp.mondomaine.be">ftp.mondomaine.be</a>	193.191.131.13

```

$TTL 3600
@      IN SOA ns.mondomaine.be.      root (
                                1      ; serial
                                10800   ; refresh
                                3600    ; retry
                                604800  ; expiry
                                3600 )  ; TTL

@      IN MX      1      relay.mondomaine.be.
@      IN NS      ns.mondomaine.be.
@      IN NS      ns.mondomaine.be.

@      IN NS      ns.mondomaine.be
ns     IN A       193.191.131.2
www   IN A       193.191.131.10
pop3  IN A       193.191.131.11
relay IN A       193.191.131.12
ftp   IN A       193.191.131.13

```

- mondomaine.be

sous domaine                    **tech.mondomaine.be** = zone  
serveur dns                      ns.mondomaine.be

dans tech.mondomaine.be

serveur web : [www.tech.mondomaine.be](http://www.tech.mondomaine.be)  
                  └ sur la machine www.mondomaine.be

```

$TTL 3600
@      IN SOA ns.mondomaine.be.      root (
                                1      ; serial

```

		10800		; refresh
		3600		; retry
		604800		; expiry
		3600	)	; TTL
@	IN	NS		ns.mondomaine.be
www	IN	CNAME		www.mondomaine.be

[ Le reste, on s'en fout ]

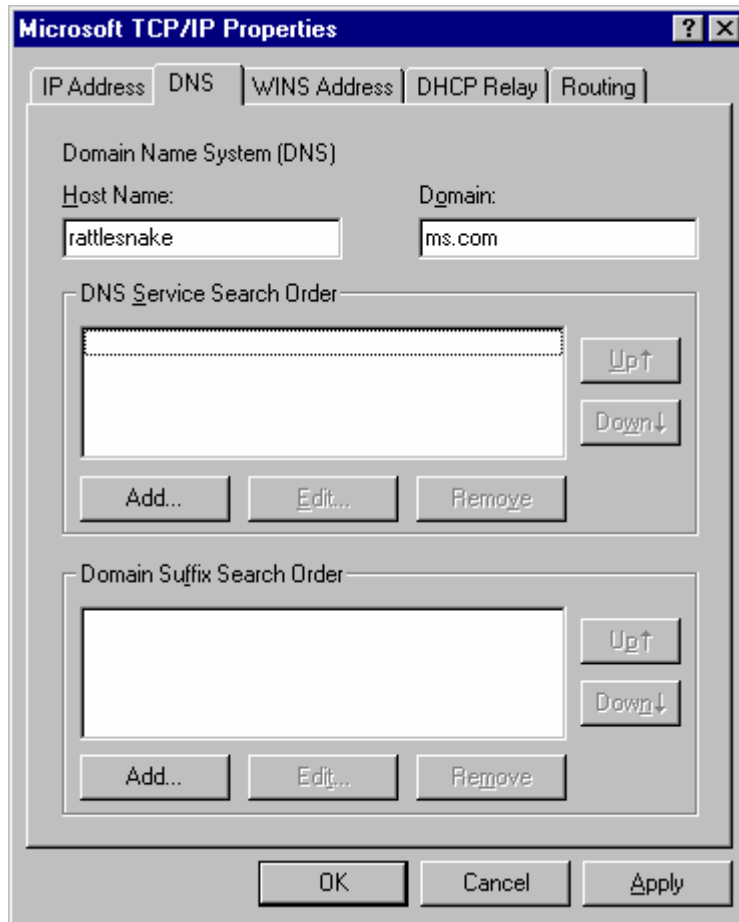
## **2. Serveur DNS sur NT serveur 4.0**

### **1. Installation du service DNS**

#### *1.1. Vérification des informations DNS sous Windows NT*

Avant d'installer le service DNS Microsoft, il est important que la pile TCP/IP du serveur Windows NT 4.0 soit correctement configurée. En particulier la section DNS a besoin d'être configurée puisque le service reçoit beaucoup de ses paramètres par défaut à partir de cette section durant son installation.

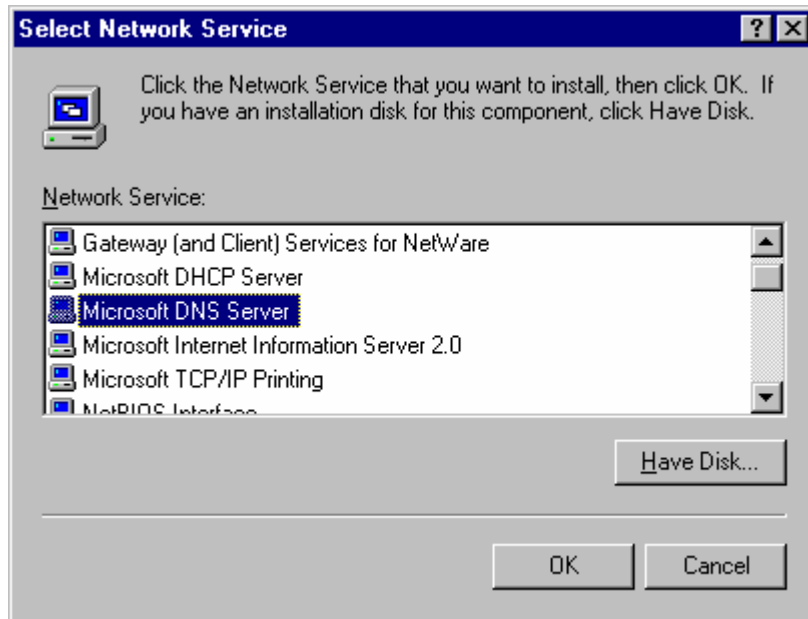
Pour vérifier ces informations, il suffit d'aller dans le panneau de configuration et de cliquer sur l'icône correspondant au réseau. Il faut alors sélectionner le protocole TCP/IP et cliquer sur le bouton propriétés et ensuite sélectionner l'onglet DNS. A ce stade, il faut vérifier que vous avez un nom d'hôte et un nom de domaine correctes.



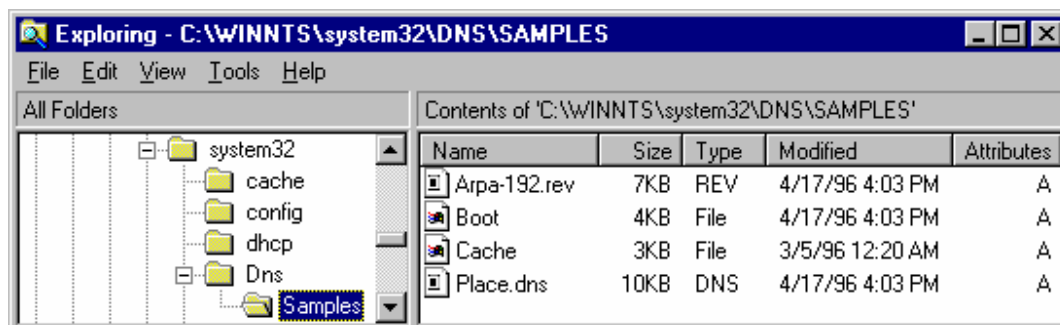
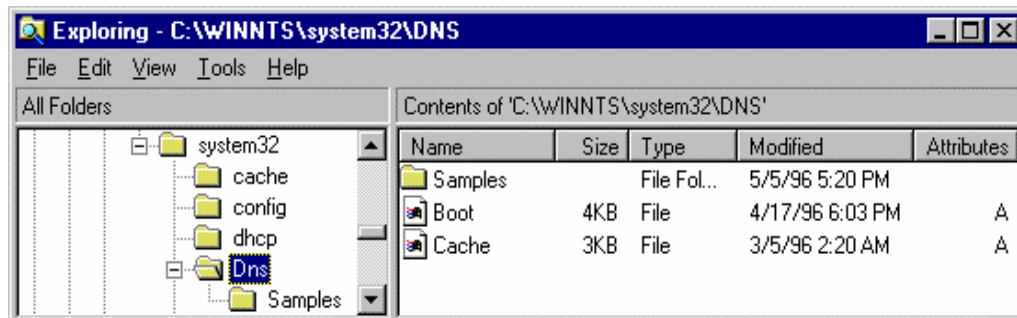
*Si le nom du domaine et le nom de l'hôte sont configurés dans le panneau de contrôle de réseau, les enregistrements SOA, A et NS seront automatiquement ajoutés lorsque une zone sera créée. Si ces informations sont manquantes, seul l'enregistrement SOA sera ajouté.*

### *1.2. Installation du service DNS Microsoft.*

Pour installer le service sur un ordinateur équipé du système d'exploitation Windows NT 4.0, il faut sous le panneau de contrôle, cliquer sur l'icône associée au réseau et sélectionner l'onglet des services. Il suffit de cliquer sur le bouton ajouter, de sélectionner le service DNS dans la liste proposée et de cliquer sur le bouton OK.



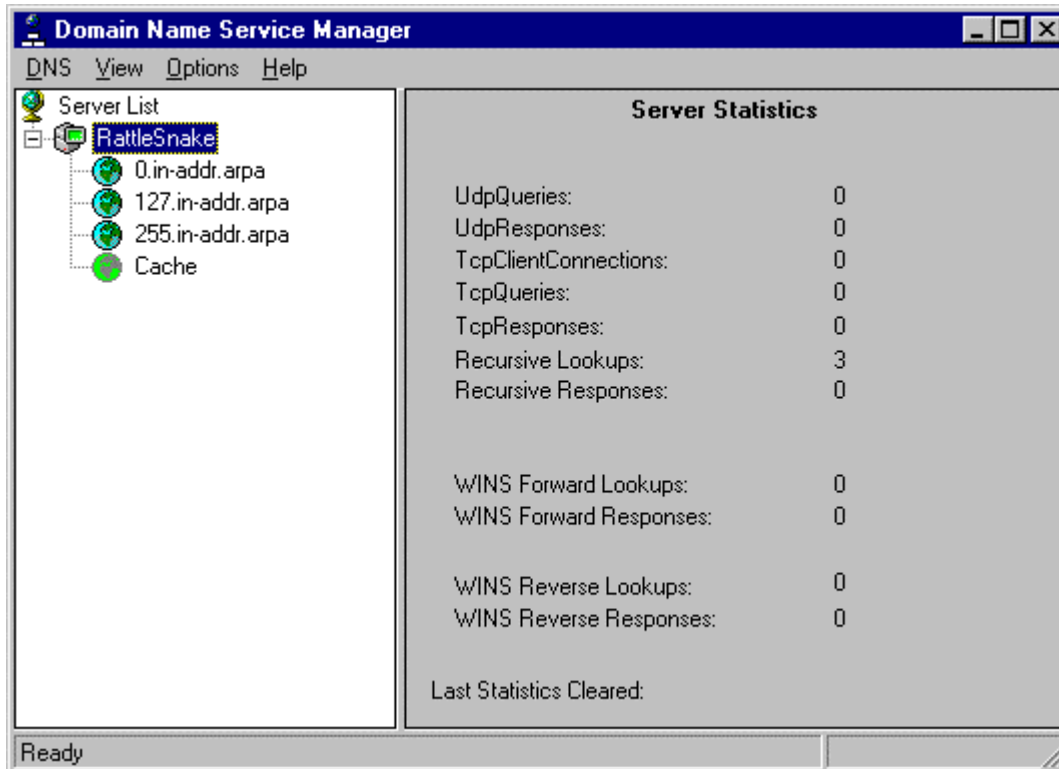
A ce stade, une installation par défaut d'un service sera effectuée. Celle-ci comprend les fichiers dans le répertoire `<SystemRoot>\system32\Dns` comme indiqué ci-après. Vous pouvez alors redémarrer votre ordinateur.



## 2. Configuration des domaines et des zones.

Pour configurer un serveur DNS, il faut utiliser le gestionnaire DNS disponible dans les outils d'administration. Initialement, le gestionnaire DNS ne comprendra aucun serveur dans sa liste. Pour ajouter

un serveur, il suffira de sélectionner l'option "Nouveau serveur" dans le menu "DNS". Il faudra entrer le nom de votre serveur local et cliquer sur le bouton OK. Le serveur apparaîtra alors dans la liste et un double clic sur ce serveur permettra de faire apparaître les statistiques de ce serveur ainsi que les zones qui y ont été définies.



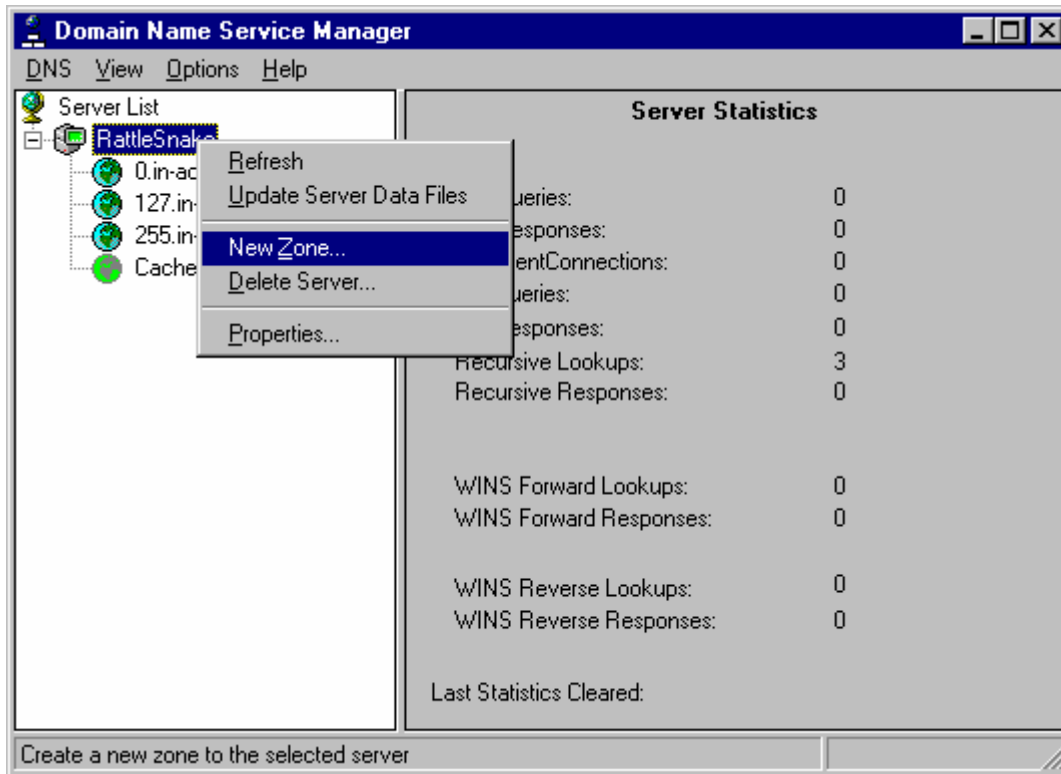
Puisque initialement le serveur n'a pas d'information à propos de son réseau spécifique, le serveur est uniquement utilisable comme serveur de cache pour l'Internet. Cela signifie que le serveur DNS contient uniquement des informations sur les serveurs racine de l'Internet.

La première étape dans la configuration d'un serveur DNS est de déterminer la hiérarchie de vos domaines DNS et de vos zones. Dès que ces informations ont été déterminées, elles peuvent alors être entrées dans votre configuration DNS en utilisant le gestionnaire DNS.

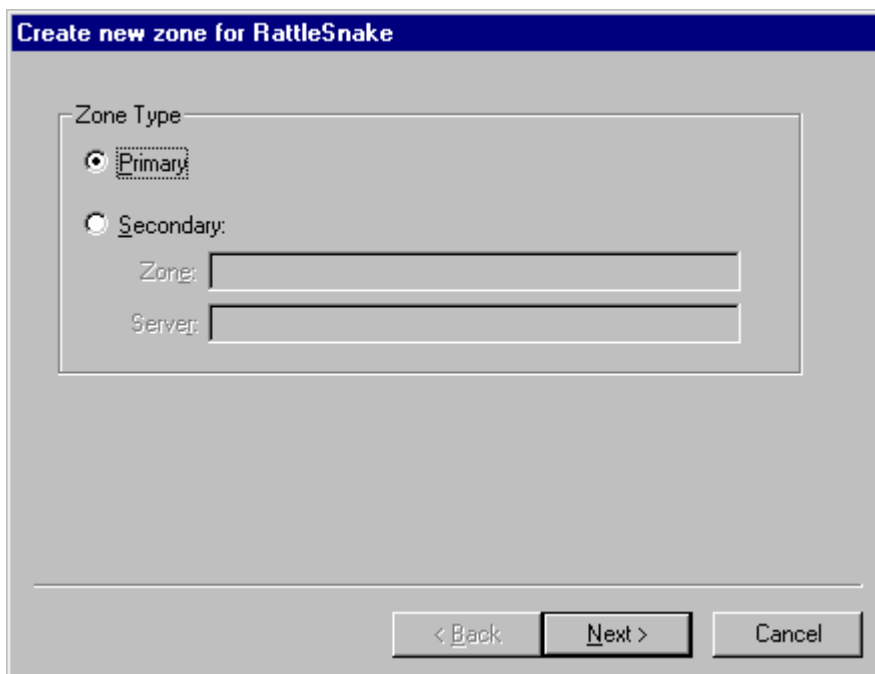
Puisque l'information DNS est groupée et contrôlée par zones, une première étape consiste à créer une zone. Pour ce faire, il suffit de cliquer sur le bouton droit de la souris sur le serveur et sélectionner alors l'option "nouvelle zone".



*Si vous double cliquez sur la zone de cache, vous pouvez voir tous les hôtes que le serveur a définis de façon statique et stockés de façon dynamique lors d'une requête précédente.*



A ce point, une boîte de dialogue apparaît vous demandant si la zone que vous créez est une zone primaire (informations stockées localement) ou une zone secondaire (informations obtenues d'un serveur maître via un transfert de zone). S'il s'agit d'une zone primaire, aucune information supplémentaire n'est nécessaire à ce stade. S'il s'agit d'une zone secondaire, vous devez entrer un nom de zone et un nom de serveur maître sur cet écran.



L'étape suivante est de remplir le nom de la zone et le nom du fichier devant contenir les informations en local sur ce serveur pour la zone renseignée. S'il s'agit d'une zone secondaire, le nom de la zone doit correspondre avec la zone sur le serveur maître. Si le fichier de zone n'existe pas encore dans le répertoire

DNS, DNS importera automatiquement les enregistrements lorsque la zone sera créée.

**Create new zone for RattleSnake**

Zone Info

Zone Name:

Zone File:

Enter the name of the zone and a name for its database.

< Back   Next >   Cancel

Si c'est une zone secondaire, vous devrez alors entrer l'adresse IP du serveur de noms maître. (Le serveur de noms avec lequel un transfert de zone sera effectué pour cette zone).

**Create new zone for CopperHead**

IP Master(s)

157.55.200.2

Add

Remove

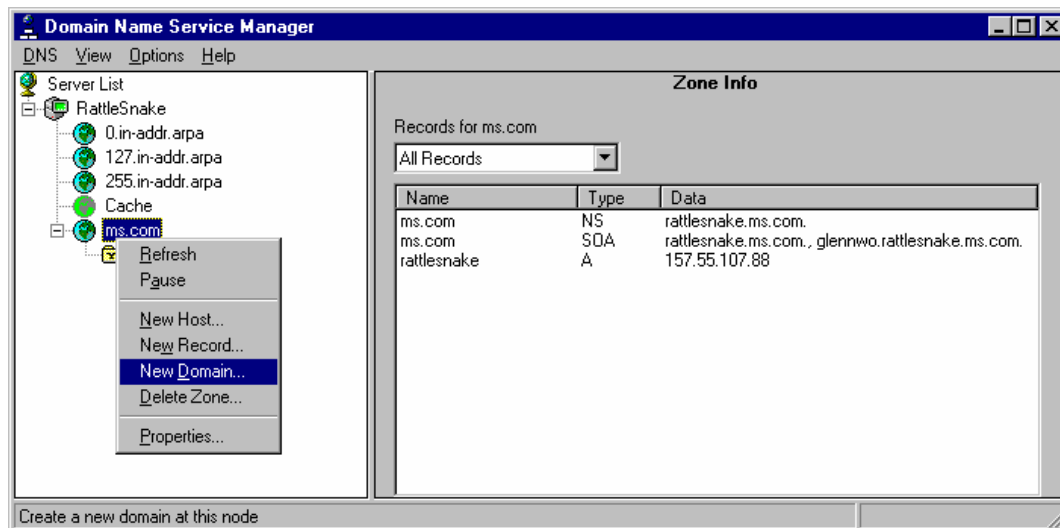
Move Up

Move Down

A secondary zone must have at least one IP Master.

< Back   Next >   Cancel

A partir du moment où toutes ces informations auront été entrées, la zone sera ajoutée dans la hiérarchie DNS. Si plusieurs zones doivent être ajoutées, il faut reprendre la même procédure pour chacune d'elles. Dès que toutes les zones ont été ajoutées, vous pouvez ajouter les sous domaines DNS que la hiérarchie doit contenir pour ces zones. Pour ce, il suffit de cliquer sur la zone souhaitée avec le bouton droit de la souris et il faut sélectionner l'option "Nouveau domaine".



Il faut alors entrer le nom du nouveau sous domaine dans la boîte de dialogue et cliquer sur le bouton OK. Ce procédé peut également être utilisé pour ajouter de nouveaux hôtes ou de nouveaux enregistrements de ressources dans la hiérarchie DNS.