Domain Name Service

1 Introduction

Le service de résolution de noms d'hôtes DNS (Domain Name Services), permet d'adresser un hôte par un nom, plutôt que par une adresse IP. Quelle est la structure d'un nom d'hôte ?

www.google.fr
machine.domaine

Le nom de domaine identifie une organisation dans l'internet, comme, par exemple, yahoo.com, wanadoo.fr, eu.org. Chaque organisation dispose d'un ou plusieurs réseaux. Ces réseaux sont composés de noeuds, ces noeuds (postes, serveurs, routeurs, imprimantes) pouvant être adressés.

Par exemple, la commande "ping www.yahoo.fr", permet d'adresser la machine qui porte le nom d'hôte "www", dans le domaine (organisation) "yahoo.fr".

Quelle différence entre la résolution de noms d'hôtes avec un serveur DNS et les fichiers "hosts" ? Avec les fichiers "hosts", chaque machine dispose de sa propre base de données de noms. Sur des réseaux importants, cette base de données dupliquée n'est pas simple à maintenir.

Avec un service de résolution de nom, la base de données est localisée sur un serveur. Un client qui désire adresser un hôte regarde dans son cache local, s'il en connaît l'adresse. S'il ne la connaît pas il va interroger le serveur de nom. Tous les grands réseaux sous TCP/IP, et Internet fonctionnent (schématiquement) sur ce principe.

Avec un serveur DNS, un administrateur n'a plus qu'une seule base de données à maintenir. Il suffit qu'il indique sur chaque hôte, quelle est l'adresse de ce serveur. Ici il y a 2 cas de figures possibles :

- soit les hôtes (clients) sont des clients DHCP (Dynamic Host Configuration Protocol). Mise à jour du dns de manière dynamique possible.

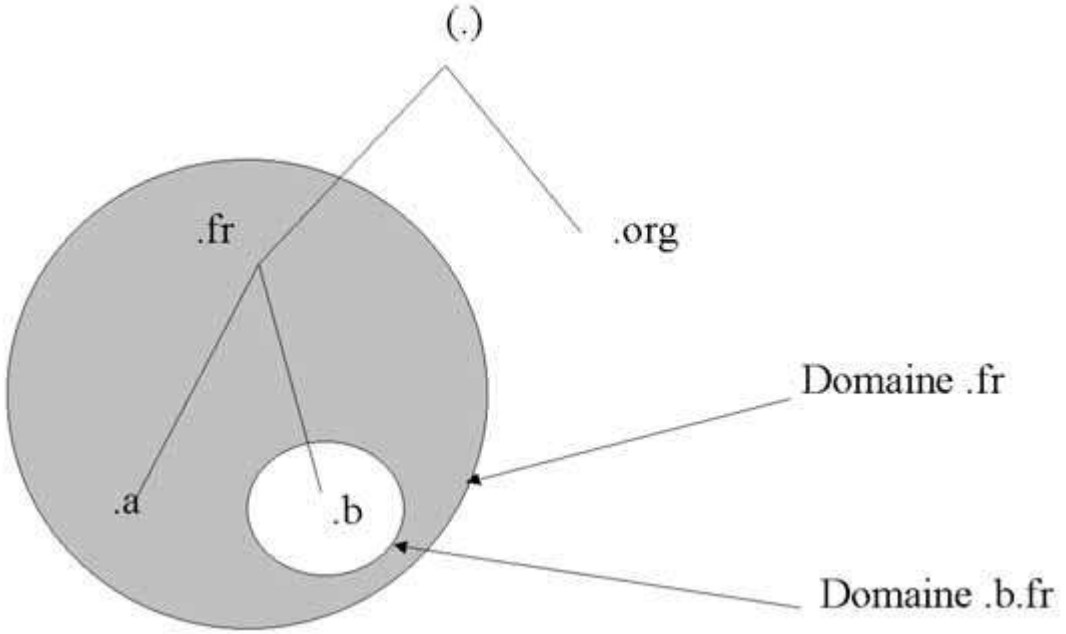
- soit les clients disposent d'une adresse IP statique. La configuration des clients est détaillée dans ce document.

Normalement un service DNS nécessite au minimum deux serveurs afin d'assurer un minimum de redondance. Les bases de données des services sont synchronisées. La configuration d'un serveur de nom secondaire sera expliquée. Nous verrons egalement en TP le fonctionnement de la réplication des bases de données bases d'enregistrements de ressources.

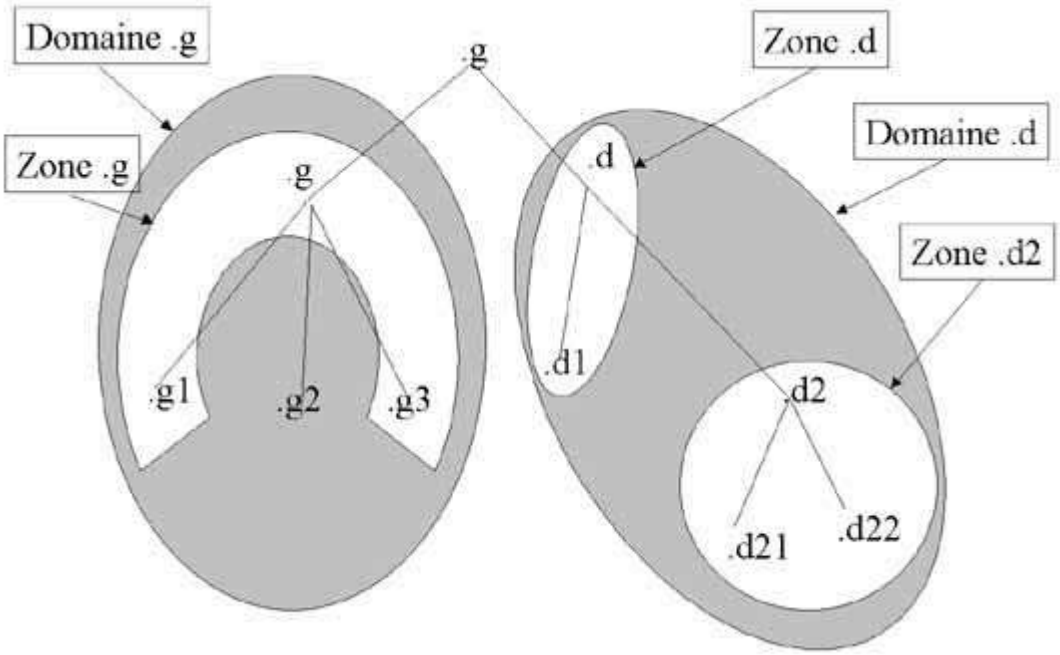
2 Présentation des concepts : notion de domaine, de zone et de délégation

Un "domaine" est un sous-arbre de l'espace de nommage. Par exemple ".com" est un domaine, il contient toute la partie hiérachique inférieure de l'arbre sous jacente au noeud ".com".

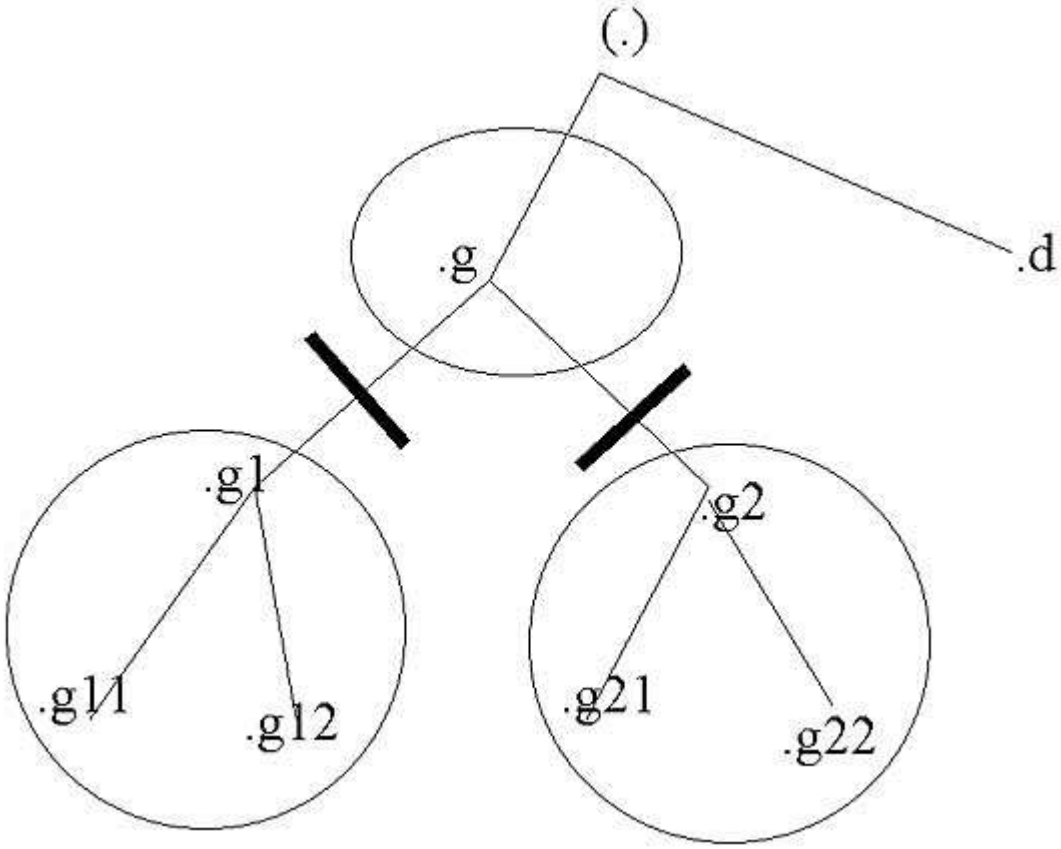
Un domaine peut être organisé en sous domaines. ".google.com" est un sous domaine du domaine ".com". Un domaine peut être assimilé à une partie ou sous-partie de l'organisation de l'espace de nommage.



Une "zone" est une organisation logique des domaines. Le rôle d'une zone est principalement de simplifier l'administration des domaines. Le domaine ".com" peut être découpé en plusieurs zones, z1.com, z2.com...zn.com. L'administration des zones sera déléguée afin de simplifier la gestion globale du domaine.



La délégation consiste à déléguer l'administration d'une zone (ou une sous-zone) aux administrateurs de cette zone.



Attention à ces quelques remarques :

- Un domaine est une organisation de l'espace de nommage. Il peut être attaché à un domaine parent, et/ou peut avoir un ou plusieurs sous-domaines enfants.

- Les zones correspondent à des organisations administratives des domaines. Un domaine peut être administré par plusieurs zones administratives, mais il est possible

aussi qu'une zone serve à l'administration de plusieurs domaines. Prenons l'exemple d'un domaine "MonEntreprise.fr", membre de ".fr". Il peut être composé de trois sous-domaines France.MonEntreprise.fr, Italie.MonEntreprise.fr, Espagne.MonEntreprise.fr et de deux zones d'administration. Une en France pour les sous-domaines France.MonEntreprise.fr, Italie.MonEntreprise.fr (il n'y a pas de délégation), et une pour Espagne.MonEntreprise.fr, il y a délégation.

- L'adressage IP correspond à une organisation physique des noeuds sur un réseau ip.

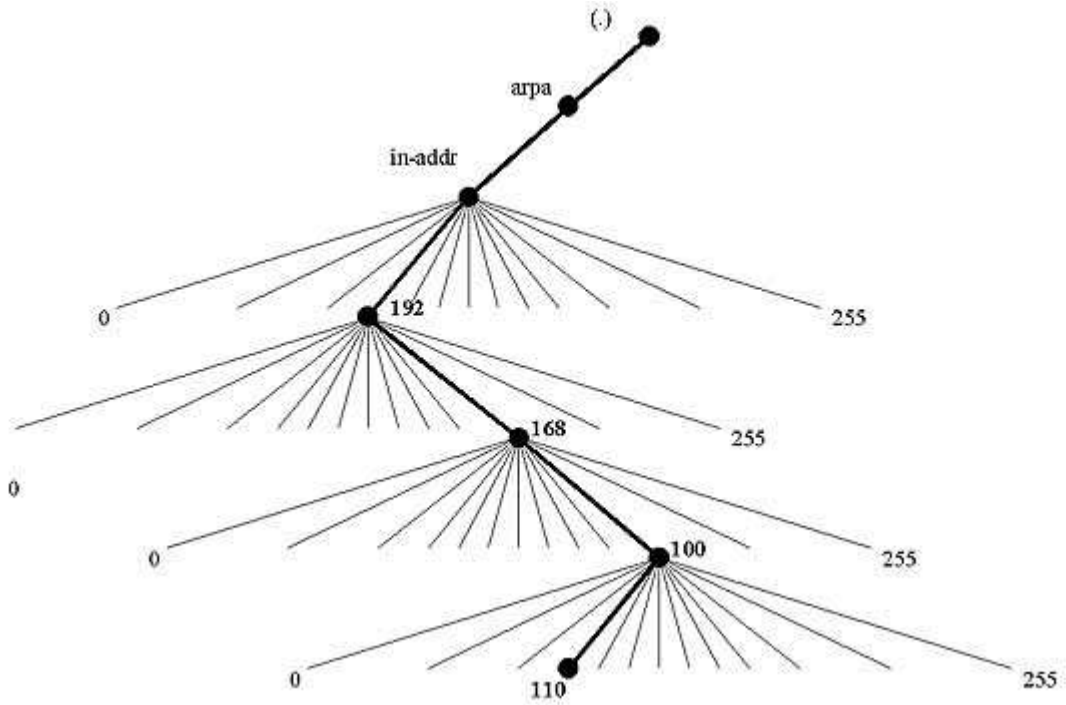
- L'organisation de l'espace de nommage est complètement indépendante de l'implantation géographique d'un réseau ou de son organisation physique.

- Les seules machines connues au niveau de l'espace de nommage, sont les serveurs de nom "déclarés".

- La cohérence (le service de résolution de nom) entre l'organisation de l'espace de nommage et les organisations physiques des réseaux sur internet et réalisées par les serveurs de noms.

3 Le domaine in-addr.arpa

Le principe de la résolution de nom, consiste à affecter un nom d'hôte une adresse IP. On parle de résolution de nom directe. Le processus inverse doit pouvoir également être mis en oeuvre. On parle de résolution de nom inverse ou reverse. Le processus doit fournir, pour une adresse ip, le nom correspondant. Pour cela il y a une zone particulière, in-addr.arpa, qui permet la résolution inverse d'adresse IP.



Par exemple, pour le réseau 192.68.1.0, on créera une zone inverse dans le domaine in-addr.arpa. La zone de recherche inverse dans le domaine deviendra : 1.68.192.in-addr.arpa. Cette zone devra répondre pour toutes les adresses déclarées dans la tranche 192.168.1.0 à 192.168.1.254.

On inscrira dans cette zone tous les noeuds du réseau pour lesquels on désire que la résolution inverse fonctionne. Un serveur de nom peut, pratiquement, fonctionner sans la définition de cette zone tant que le réseau n'est pas relié à l'internet. Si cela était le cas, il faudrait déclarer cette zone, sans quoi, des services comme la messagerie électronique, ne pourrait fonctionner correctement, notamment à causes des règles anti-spam. (Voir www.nic.fr)

4 Fichiers, structure et contenus

Sur linux nous allons utiliser deux types de fichiers :

- le fichier /etc/bind/named.conf, qui décrit la configuration générale du serveur dns

- les fichiers qui contiennent les enregistrements de ressources pour la zone dans / var/named.

Les enregistrements ont une structure et un rôle.
Principaux types d'enregistrements
Les types d'enregistrements qui enrichissent une base de données DNS sont de plusieurs types, dont voici les principaux:

- Enregistrement de type SOA (Start Of Authority) : Indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations pour le domaine, par exemple le

délai de mise à jours des bases de données entre serveurs de noms primaires et secondaires, le nom du responsable du site.
- Enregistrements de type NS (Name Server) : Ces enregistrements donnent les adresses des serveurs de noms pour le domaine.
- Enregistrement de type A (Adresse) : Ces enregistrements permettent de définir les noeuds fixes du réseau (ceux qui ont des adresses ip statiques). Serveurs, routeurs, switchs?
- Enregistrements de type MX (Mail eXchanger) : Ils servent pour déclarer les serveurs de messagerie.
- Enregistrements de type CNAME (Canonical Name) : Ils permettent de définir des alias sur des noeuds existants.
- Enregistrement de type PTR (Pointeur) : Ils permettent la résolution de nom inverse dans le domaine in-addr.arpa.

Ces enregistrements caractérisent des informations de type IN - INternet. Voir l'annexe pour avoir un fichier exemple.

Structure des enregistrements

Strucure d'un enregistrement SOA : Chaque fichier commence par un enregistrement de type SOA. Voici un exemple d'enregistrement SOA.

```
foo.org. IN SOA ns1.foo.org. hostmaster.foo.org. (
        20001210011     ; numéro de série
        10800           ; rafaîchissement
        3600            ; nouvel essai
        604800          ; Obsoléscence après une semaine
        86400 )         ; TTL minimal de 1 jour
```

Caractéristiques des différentes informations :
SOA Start Of Authority, enregistrement qui contient les informations de synchronisation des différents serveurs de nom.
foo.org, donne le nom de la zone.
hostmaster.foo.org : la personne qui est responsable de la zone. Le premier point sera remplacé par l'arobase (@) pour envoyer un courrier électronique. En général postmaster, est une alias de messagerie électronique vers l'administrateur du DNS. Cela deviendra hostmaster@foo.org.

1. Numéro de série sous la forme AAAAMMJJNN, sert à identifier la dernière modification sur le serveur de nom maître. Ce numéro sera utilisé par les serveurs de nom secondaires pour synchroniser leurs base. Si le numéro de série du serveur de nom primaire est supérieur à celui des serveurs de noms secondaire, alors le processus de synchronisation suppose que l'administrateur à apporté une modification sur le serveur maître et les bases sont synchronisées.
2. Rafraîchissement : Intervalle de temps donné en seconde pour indiquer au serveur la période de test de la validité de ses données.
3. Retray : Intervalle de temps avant réïtération si l'essai précédent n'a pas fonctionné.
4. Expire : Temps au bout duquel le serveur ne remplit plus sa mission s'il n'a pu contacter le serveur maître pour mettre à jour ses données.
5. TTL : Time To Live, durée de vie des enregistrements. Plus la durée de vie est courte, plus l'administrateur est susceptible de considérer que ses bases sont à jour, par contre cela augmente le traffic sur le réseau.

Enregistrement de type NS pour le domaine foo.org:

```
foo.org.        IN NS   ns1.foo.org.
foo.org.        IN NS   ns2.foo.org.
```

Enregistrements de type A : Nous devons décrire la correspondance Nom / Adresse

```
ns1.foo.org.          IN      A       192.168.0.1
ns2.foo.org.          IN      A       192.168.0.2
localhost.foo.org.    IN      A       127.0.0.1
```

S'il y avait d'autres hôtes sur la zone, il faudrait les définir ici.
Enregistrements de type CNAME *:* Ce sont les alias (Canonical Name). Une requête du type

http://www.foo.org sera adressée à ns1.foo.org, puisque www est un alias de ns1.

```
ns1.foo.org.    IN      CNAME   www.foo.org.
ns2.foo.org.    IN      CNAME   ftp.foo.org.
```

Enregistrement de type PTR *:* Il serviront à la résolution de nom inverse.

```
1.0.168.192.in-addr.arpa.       IN      PTR     ns1.foo.org.
2.0.168.192.in-addr.arpa.       IN      PTR     ns2.foo.org.
```

La délégation

La délégation consiste à donner l'administration d'une partie du domaine à une autre organisation. Il y a transfert de responsabilité pour l'administration d'une zone. Les serveurs de la zone auront autorité sur la zone et auront en charge la responsabilité de la résolution de nom sur la zone. Les serveurs ayant autorité sur le domaine auront des pointeurs vers les serveurs de noms ayant autorité sur chaque zone du domaine.

Serveur primaire et serveur secondaire

Le serveur maître (primaire) dispose d'un fichier d'information sur la zone. Le ou les serveurs esclaves (secondaires) obtiennent les informations à partir d'un serveur primaire ou d'un autre serveur esclave. Il y a transfert de zone. Les serveurs maîtres et esclaves ont autorité sur la zone.

Le cache

L'organisation d'internet est assez hiérarchique. Chaque domaine dispose de son propre serveur de nom. Chaque zone de niveau supérieur (edu, org, fr...) dispose également de serveurs de nom de niveau supérieur. Le service DNS installe une liste de serveurs de noms de niveaux supérieurs. Cette liste permet à votre serveur de résoudre les noms qui sont extérieurs à votre zone. Le serveur enrichit son cache avec tous les noms résolus. Si votre réseau réseau n'est pas relié à internet, vous n'avez pas besoin d'activer cette liste.

Ce fichier est un peu particulier. Il est fournit avec les distributions. Il est utilisé par le serveur de nom à l'initialisation de sa mémoire cache. Si vos serveurs sont raccordés à internet, vous pourrez utiliser une liste officielle des serveurs de la racine (ftp.rs.internic.net).

Installation d'un serveur DNS

Processus d'installation

Pour mettre en place le service de résolution de nom sur un serveur Linux, on va procéder successivement aux opérations suivantes :

1. installer le package si cela n'est pas déjà réalisé,
2. configurer les fichiers,
3. démarrer le service serveur.

Installer le package

La résolution de nom est réalisée par les produits du package bind. La version actuelle est le package bind-9.x. qui remplace les versions antérieures 4.x. Dans cette version, de nombreuses modifications ont été apportées surtout au niveau de la sécurité, mais également en ce qui concerne le service DNS dynamique, c'est à dire acceptant les inscriptions des clients DHCP. La compatibilité ascendante est respectée. Nous resterons sur une configuration simple.

On va utiliser "bind 9". Il faudra donc installer les fichiers bind-9.x et bind-utils-9.x. Ce deuxième package donne quelques outils comme host, nslookup... Pour installer utilisez la commande : mount /mnt/cdrom;rpm -i /mnt/cdrom/RedHat/rpms/bind-9*.rpm

Procédure de configuration du serveur

L'installation a copié les fichiers. Sur une configuration simple vous allez avoir 5 fichiers à créer ou à modifier sur le serveur primaire :

- /etc/named.conf (fichier de configuration global du service DNS du serveur de nom primaire),
- /var/named/master/stage.org qui contiendra la description de la correspondance nom-adresse de toutes les machines du réseau
- /var/named/master/1.168.192 qui contiendra la correspondance inverse adresse-nom (pour la résolution inverse de nom in-addr.arpa)
- un fichier /var/named/master/localhost pour la configuration locale (localhost - 127.0.0.1).
- un fichier /var/named/master/0.0.127 pour la configuration reverse (127.0.0.1 - localhost).

Si le serveur était relié à internet ou faisait office de serveur officiel, il y aurait d'autres fichiers à configurer.

Configurer les fichiers

Le fichier racine pour la configuration du serveur de nom est le fichier "/etc/named.conf". Ce fichier est lu au démarrage du service et donne la liste des fichiers qui définissent la base de données pour la zone. La distribution donne un script perl qui permet de transcrire un fichier named.boot (bind version 4) au format named.conf (BIND version 9). Pour générer named.conf à partir de named.boot (si vous utilisiez une ancienne version de bind, par exemple), vous pouvez utiliser le script Perl named-bootconf qui est dans /usr/doc/bind-9

Le fichier named.conf

Voici un exemple de fichier commenté pour le domaine fictif stage.org, d'adresse 192.168.1.0.

```
#fichier named.conf pour le domaine stage.org
#Indication du chemin où sont localisés les fichiers de la base de données

options {
directory       "/var/named";
};

#pour le fichier de cache du serveur de nom

zone "." in {
        type hint;
        file "named.ca";
};


#pour la recherche directe dans le domaine, serveur primaire, on utilise le fichier
#/var/named/master/stage.org

zone "stage.org" in {
        type master;                    # nous sommes serveur primaire de ce domaine
        file "stage";                   # fichier contenant les correspondances nom, adresse IP
};

# pour la recherche de zone inverse (reverse) on utilise le fichier 1.168.192

zone "1.168.192.in-addr.arpa" in {
        type master;                    # nous sommes serveur primaire de ce domaine aussi
        file "1.168.192";
};

#pour la résolution de nom sur localhost

zone "local" in {
        type master;                    # nous sommes serveur primaire de ce domaine
        file "localhost";               # fichier contenant les correspondances nom, adresse IP
};

# rappel : la machine locale porte toujours l'adresse « localhost » 127.0.0.1
# nous proposons donc la résolution inverse sur cette zone ?
#la description est dans /var/named/master/0.0.127

zone "0.0.127.in-addr.arpa" in {
        type master;                    # nous sommes également serveur primaire de ce domaine
        file "0.0.127";
};
```

Notez bien que les noms appliqués aux fichiers de ressources ne sont en rien imposés. Il s'agit d'une pure convention. En effet un serveur de nom peut prendre en charge plusieurs domaines, cela permet de structurer l'organisation des fichiers de ressources.
Notez également l'option "type master". Il s'agit d'un serveur primaire. Nous verrons comment déclarer un serveur secondaire.

Le fichier /var/named/master/stage.org

Le paramètre @, signifie qu'il s'agit du domaine "stage.org" (le nom tapé après le mot « zone » dans le fichier de configuration named.conf). Le paramètre "IN", signifie qu'il s'agit d'un enregistrement de type Internet. Notez la présence d'un point (.) après le nom des machines. Sans celui-ci, le nom serait « étendu ». Par exemple, ns1.stage.org (sans point) serait compris comme ns1.stage.org.stage.org (on rajoute le nom de domaine en l'absence du point terminal). Le point (.) terminal permet de signifier que le nom est pleinement qualifié.

```
; NB : dans ces fichiers, les commentaires sont précédés d'un point-virgule.
; enregistrement de type SOA, on déclare tous les paramètres
; ainsi que l'adresse du responsable administratif de la zone, ici : postmaster

$TTL        3h
@           IN          SOA         ns1.stage.org. postmaster.stage.org. (
                        16      ; ces nombres ne sont pas expliqués ici
                        86400   ; vous pouvez les employer tels quels
                        3600    ; sans problème tant que vous ne mettez
                        3600000 ; pas en place un serveur de nom
                        604800  ; secondaire. )
; enregistrement de type Name Server, on déclare le serveur de nom
IN          NS          ns1.stage.org.

; on déclare les autres noeuds pour la résolution de nom
; Notez l'absence du point après les noms pour permettre « l'extension » du nom de domaine.
ns1         IN          A           192.168.1.1
; ici un client
cli1        IN          A           192.168.1.2

; on déclare les alias CNAME.  La machine proc sert de serveur de messagerie, Web, FTP, news et DNS.
mail        IN          CNAME   ns1
news        IN          CNAME   ns1
www         IN          CNAME   ns1
ftp         IN          CNAME   ns1
```

Le fichier /var/named/master/localhost

```
$TTL        3h
@           IN          SOA         ns1.stage.org. postmaster.stage.org. (
                        16      ; ces nombres ne sont pas expliqués ici
                        86400   ; vous pouvez les employer tels quels
                        3600    ; sans problème tant que vous ne mettez
                        3600000 ; pas en place un serveur de nom
                        604800  ; secondaire. )

; enregistrement de type Name Server
IN          NS          ns1.stage.org.

;On déclare le noeud dans le domaine local
localhost           IN          127.0.0.1
```

Le fichier /var/named/master/1.168.192

Ici il s'agit de la résolution de nom inverse de la zone stage.org.

```
$TTL        3h
```

```
@           IN          SOA         ns1.stage.org. postmaster.stage.org. (
                        16      ; ces nombres ne sont pas expliqués ici
                        86400   ; vous pouvez les employer tels quels
                        3600    ; sans problème tant que vous ne mettez
                        3600000 ; pas en place un serveur de nom
                        604800  ; secondaire. )

; enregistrement de type Name Server
            IN          NS          ns1.stage.org.

;On déclare les noeuds dans le domaine 1.168.192.in-addr.arpa
; Ici, on ne peut pas se passer du nom complet (fini par un point).
;l'extension serait (exemple avec ns1) : 1.1.168.192.in-addr.arpa.
1           IN          PTR         ns1.stage.org.
```

Le fichier /var/named/master/0.0.127

Ce fichier assure la résolution pour 1.0.0.127.in-addr.arpa

```
$TTL        3h
@           IN          SOA         ns1.stage.org. postmaster.stage.org. (
                                    16      ; ces nombres ne sont pas expliqués ici
                                    86400   ; vous pouvez les employer tels quels
                                    3600    ; sans problème tant que vous ne mettez
                                    3600000 ; pas en place un serveur de nom
                                    604800  ; secondaire. )
)

; enregistrement de type Name Server
            IN          NS          ns1.stage.org.

;On déclare les noeuds dans le domaine 0.0.127.in-addr.arpa
; Normalement, il n'y en a qu'un : 127.0.0.1 = localhost.
; Noter le point terminal.
1           IN          PTR         localhost.
```

Compléments pratiques

Démarrer ou arrêter le service le service

Le service (daemon) qui active la résolution de nom s'appelle "named", prononcer "naime dé".

Si vous voulez l'arrêter ou le redémarrer dynamiquement vous pouvez utiliser les commandes suivantes :

/etc/rc.d/init.d/named stop

/etc/rc.d/init.d/named start

Relancer le service serveur de cette façon peut parfois poser problème. En effet cette procédure regénère le cache du serveur. Le service prends également un nouveau "PID". Si vous voulez éviter cela, ce qui est généralement le cas, préférez la commande "kill -HUP 'PID de Named'". Vous trouverez le PID de named dans "/var/run".

Finaliser la configuration

Les fichiers de configuration sont créés. Il ne reste plus qu'à tester. Il faut au préalable configurer le serveur pour qu'il utilise lui même le service DNS et redémarrer les services réseau. Relancez, ensuite le service réseau. Utilisez les commandes suivntes :

/etc/rc.d/init.d/network stop

/etc/rc.d/init.d/network start

Procédure de configuration du client

La description de la configuration de tous les clients possibles n'est pas détaillée. Vous trouverez ci-dessous des éléments pour un client windows 9x et pour un client Linux.

Avec Windows

Il s'agit d'un client Windows. Chaque client dispose du protocole TPC/IP, d'une adresse IP. Il

faut configurer le client pour lui signifier quel est le serveur de nom qu'il doit consulter. Pour cela il faut aller dans : panneau de configuration - réseau - tcp/ip - Onglet "Configuration DNS". Vous allez pouvoir définir les paramètres suivants

- le nom d'hôte de la machine locale dans le réseau
- le nom de domaine auquel appartient l'hôte (dans cet exemple c'est stage.org)

Ces 2 paramètres sont facultatifs dans l'atelier qui nous intéresse. Par contre le paramètre "Ordre de recherche DNS" est important. Mettez dessous :

- L'adresse IP du serveur de nom que vous avez configuré,
- Cliquez sur ajouter
- Entrez l'adresse ip du serveur de nom
- Validez puis relancer la machine

Ce paramètre, définit à la machine locale, l'adresse de l'hôte de destination qui est chargé de la résolution des noms d'hôtes dans le réseau. Cela permet de dire qu'un serveur de nom doit avoir une adresse IP statique sur le réseau.

Avec Linux

Vous pouvez utiliser linuxconf (cf.plus haut) ou bien modifier (en tant que « root ») le fichier de configuration du « resolver » (/etc/resolv.conf).

```
# Fichier /etc/resolv.conf
search stage.org
nameserver 192.168.1.1 # mettre votre DNS
```

/etc/bind/named.conf

```
 //
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//

options {
	directory "/var/cache/bind";


	// forwarders {
	//	0.0.0.0;
	// };

	auth-nxdomain no;	# conform to RFC1035
};

// prime the server with knowledge of the root servers
zone "." {
	type hint;
	file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
	type master;
	file "/etc/bind/db.local";
};
```

```
// add entries for other zones below here

zone "dnc" {
	type master;
	file "/var/cache/bind/dnc.hosts";
	allow-update {
		127.0.0.1;
	};
};

zone "1.168.192.in-addr.arpa" {
	type master;
	file "/var/cache/bind/192.168.1.rev";
	allow-update {
		127.0.0.1;
	};
};
```

/etc/bind9/dhcp.conf

```
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
update-static-leases on;
ddns-domainname "dnc";

default-lease-time 600;
max-lease-time 7200;

option domain-name-servers 192.168.1.10;
option subnet-mask 255.255.255.0;
option routers 192.168.1.1;

log-facility local7;

subnet 192.168.1.0 netmask 255.255.255.0 {
	range 192.168.1.200 192.168.1.210;
	allow unknown-clients;
}

zone dnc. {
   primary 127.0.0.1;
}

zone 1.168.192.in-addr.arpa. {
   primary 127.0.0.1;
}
```