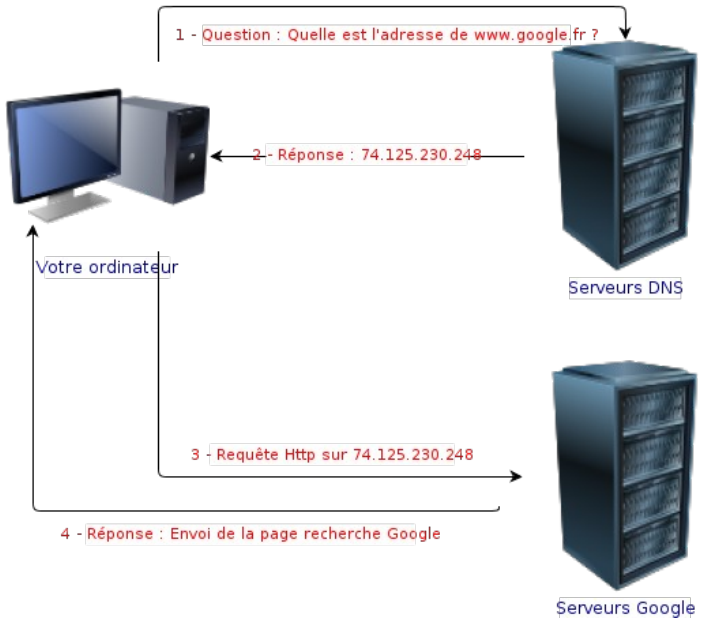
Annexe – Service DNS
Domain Name System

Sommaire :

I - Introduction

DNS signifie **Domain Name System**. un serveur **DNS** est un **annuaire** pour ordinateur qui réalise la **résolution de noms** consistant à fournir une **adresse IP** pour un **nom d'hôte**. Lorsque vous voulez accéder à un ordinateur dans le réseau, votre ordinateur va interroger le serveur **DNS** pour récupérer l'**adresse IP** de l'ordinateur que vous voulez joindre. Une fois, que votre ordinateur aura récupéré l'adresse du destinataire, il pourra le joindre directement avec son **adresse IP**.

Principe d'une requête DNS



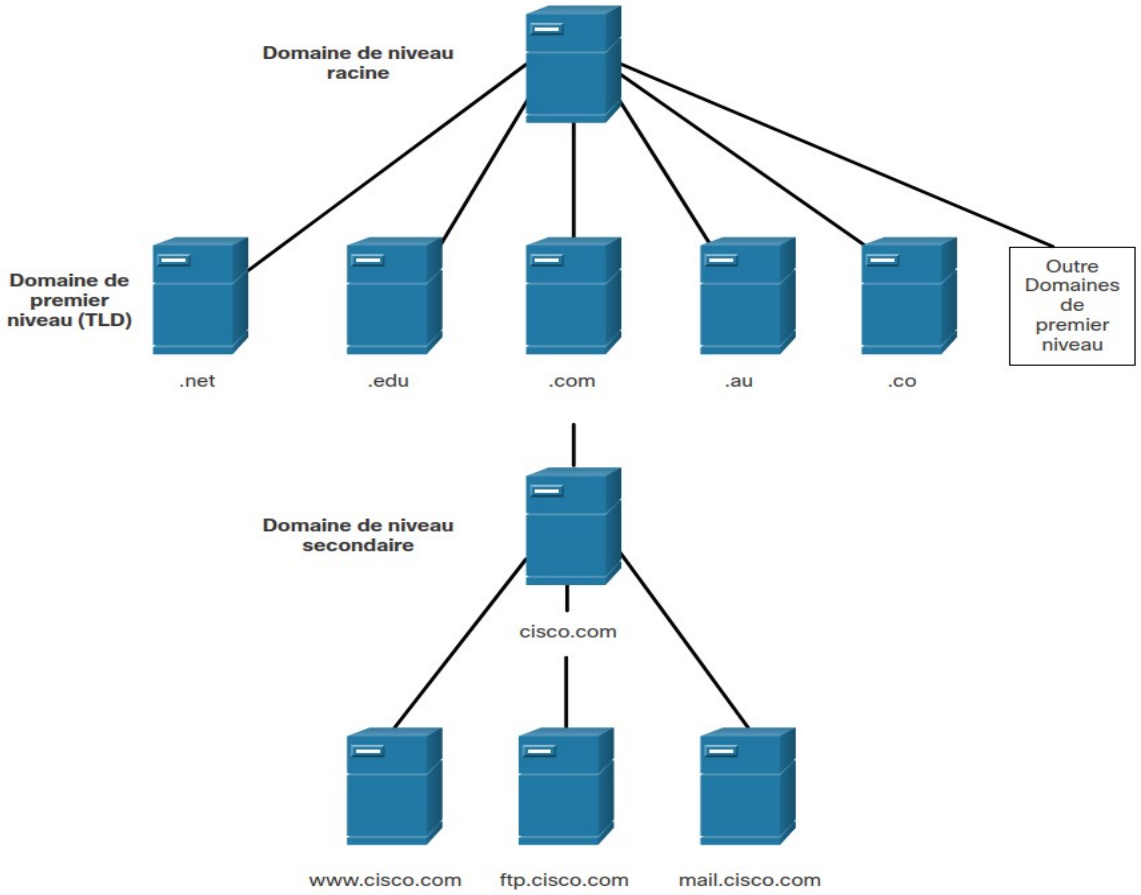
DNS utilise le protocole **UDP** et le port **53** pour les requêtes et les réponses **DNS**. Les requêtes DNS sont envoyées par un client et les réponses sont émises par des serveurs DNS.

Les serveurs **DNS** fonctionnent en **cascade**. Lorsqu'un serveur ne connaît pas la réponse, il va demander à son « **parent** ». A la maison, ce serveur est la box, et si la box ne sait pas répondre, elle va interroger son parent : le(s) serveur(s) **DNS** de votre **fournisseur d'accès**. Cela peut remonter comme ça jusqu'aux serveurs **DNS racines**. On va dire pour simplifier que les serveurs **DNS racines** sont les serveurs de base du système : on ne peut pas remonter plus haut.

II - Notions de domaines et de zones

II.1. Hiérarchie des domaines DNS

Un "**domaine**" est un sous-arbre de l'espace de nommage. Le **DNS** se compose d'une hiérarchie de **domaines** génériques de **premier niveau** qui incluent les domaines **.com**, .**net**, **.org**, **.gov**, **.edu** et de nombreux domaines nationaux, tels que **.br** (Brésil), **.es** (Espagne), **.uk** (Royaume-Uni), etc. Le niveau suivant de la hiérarchie DNS comprend les **domaines de second niveau**. Ils sont représentés par un nom de domaine suivi d'un domaine de premier niveau. Les sous-domaines composent le niveau suivant de la hiérarchie DNS et représentent en quelque sorte une division des domaines de second niveau. Enfin, un quatrième niveau peut représenter un hôte dans un sous-domaine



II.2. Zone

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

II.3. Domaine in-addr.arpa

Le principe de la **résolution de noms**, consiste à affecter un **nom d'hôte** à une **adresse IP**, on parle de **résolution de noms directe**. Le processus inverse doit pouvoir également être mis en œuvre. On parle de **résolution de noms inverse** ou **reverse**. Le processus doit fournir, pour une **adresse IP**, le **nom d'hôte** 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 **192.168.2.0**, on créera une zone inverse dans le domaine **in-addr.arpa**. La zone de recherche inverse dans le domaine deviendra : **2.168.192.in-addr.arpa**. Cette zone devra répondre pour toutes les adresses déclarées dans la tranche **192.168.2.1** à **192.168.2.254**.

III - Installation et configuration du service DNS

III.1. Installation du service DNS

Plusieurs **serveurs DNS** sont disponibles, on va installer le serveur DNS de référence nommé **BIND** dans sa version **9** (**B**erkeley **I**nternet **N**ame **D**omain). Pour cela Il faut installer le package **bind9** en exécutant la commande :

apt-get install bind9

III.2. Configuration du service DNS

Les fichiers de configuration de **bind** se trouvent dans le dossier ***/etc/bind***. La configuration du serveur DNS consiste à renseigner **2 types de fichiers** :

- le fichier ***/etc/bind/named.conf***, qui décrit la configuration générale du serveur DNS. Ce fichier est lu au démarrage du service et donne la liste des fichiers qui définissent la base de données pour la zone. Ce fichier inclut les fichiers :
  - ***/etc/bind/named.conf.options*** qui définit les autres serveurs DNS à contacter avec l'option ***forwarders*** ;
  - ***/etc/bind/named.conf.local*** qui décrit la configuration locale ;
  - ***/etc/bind/named.conf.default-zones*** qui décrit la configuration locale des zones.

- les fichiers qui contiennent les **enregistrements** de ressources pour la zone utilisée dans ***/etc/bind***. On retrouve au minimum les 2 fichiers suivants :
  - ***/etc/bind/db.mondomaine*** qui contiendra la description de la correspondance nom-adresse de toutes les machines du domaine ***mondomaine*** ;
  - ***/etc/bind/db.192.168.7.hosts*** qui contiendra la correspondance inverse adresse-nom (pour la résolution inverse de nom **in-addr.arpa)** pour le réseau d'adresse **192.168.7.0/24**.

III.3. Principaux types d'enregistrements

Les **types d'enregistrements** qui enrichissent une base de données **DNS** sont de plusieurs types :

- Enregistrement de type **SOA** (**S**tart **O**f **A**uthority) : Indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations sur le domaine.

- Enregistrements de type **NS** (**N**ame **S**erver) : Ces enregistrements donnent les adresses des serveurs de noms pour le domaine.

- Enregistrement de type **A** (**A**dresse) : Ces enregistrements permettent de définir les nœuds fixes du réseau (ceux qui ont des adresses IP statiques). Serveurs, routeurs.

- Enregistrements de type **MX** (**M**ail e**X**changer) : Ils servent pour déclarer les serveurs de messagerie.

- Enregistrements de type **CNAME** (**C**anonical **NAME**) : Ils permettent de définir des alias sur des nœuds existants.

- Enregistrement de type **PTR** (**P**oin**T**eu**R**) : Ils permettent la résolution de noms inverse dans le domaine **in-addr.arpa**.

Tous ces enregistrements caractérisent des informations de type **IN** – **In**ternet.

III.4. Structure des enregistrements

*3.4.1 : Structure d'un enregistrement **SOA** :*

Chaque fichier commence par un enregistrement de type **SOA**.

@ IN SOA monserveur.mondomaine. root.monserveur.mondomaine. (
2022022700 ; numéro de série (Serial)
10800 ; Mise à jour toutes les 3 H (Refresh)
3600 ; nouvel essai dans 1 H (Retry)
604800 ; Expire au bout de 7 jours (Expire)
86400) ; TTL minimal de 1 jour = 24 H

Caractéristiques des différentes informations :

- **SOA** Start Of Authority, enregistrement qui contient les informations de synchronisation des différents serveurs de nom. **@**, donne le nom de la zone.

- **root.myserver.mydomain** : la personne qui est responsable de la zone.

- **Serial** : Numéro de série sous la forme **AAAAMMJJNN**, sert à identifier la dernière modification sur le serveur de noms maître. Ce numéro sera utilisé par les serveurs de nom secondaires pour synchroniser leurs bases. Si le numéro de série du serveur de noms 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.

- **Refresh** : Intervalle de temps donné en seconde pour indiquer au serveur la période de test de la validité de ses données.

- **Retry** : Intervalle de temps avant réitération si l'essai précédent n'a pas fonctionné.

- **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.

- **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 trafic sur le réseau.

*3.4.2 : Structure d'un enregistrement de type **NS** :*

mondomaine. IN NS ns1.mondomaine.
mondomaine. IN NS ns2.mondomaine.

*3.4.3 : Structure d'un enregistrement de type **A** :*

Nous devons décrire la correspondance Nom / Adresse.

ns1.mondomaine. IN A 192.168.0.1
ns2.mondomaine. IN A 192.168.0.2
localhost. mondomaine. IN A 127.0.0.1

S'il y a d'autres hôtes sur la zone, il faut les définir ici.

*3.4.4 : Structure d'un enregistrement de type **CNAME** :*

Ce sont les alias (**C**anonical **NAME**). Une requête du type **http://www.mondomaine** sera adressée à **ns1.mondomaine**, puisque **www** est un alias de **ns1**.

www IN CNAME ns1.mondomaine.

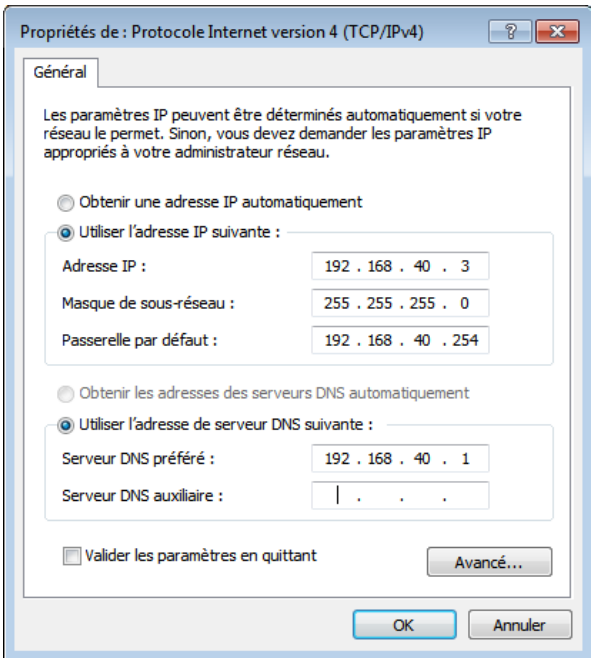
*3.4.5 : Structure d'un enregistrement de type **PTR** :* Il serviront à la résolution de noms inverse.

1.2.16.172.in-addr.arpa. IN PTR ns1.mondomaine.
2.2.16.172.in-addr.arpa. IN PTR ns2.mondomaine.

III.5. Configuration du client DNS

3.5.1 : Client Windows

Il suffit de modifier les **propriétés** du **protocole TCP/IPv4** en spécifiant l'adresse du serveur **DNS** :



Pour visualiser la configuration réseau (en ligne de commande), on utilise la commande **ipconfig /all**.
Pour libérer l'interface réseau, on utilisera la commande **ipconfig /release**.
Pour renouveler l'interface réseau, on utilisera la commande **ipconfig /renew**.
On peut taper **ipconfig /?** pour voir comment utiliser la commande **ipconfig**.

3.5.2 : Client Linux

Si le poste n'est pas client DHCP, il suffit de modifier manuellement la configuration du client en modifiant le contenu du fichier ***/etc/resolv.conf***. Il faut préciser dans ce fichier le nom du domaine de recherche ainsi que l'adresse du serveur DNS.

Lorsque la modification est effectuée, il faut relancer le service réseau. En exécutant la commande **service networking restart**.

Exemple de fichier **/etc/resolv.conf** :

search mondomaine
nameserver 172.16.2.1

III.6. Test du service DNS

Le test du serveur **DNS** peut se faire avec l'utilitaire **host**.

3.6.1 : Liste des machines du domaine mondomaine

host –l mondomaine

mondomaine name serveur-linux-40 serveur-linux-40.mondomaine.
serveur-linux-40.mondomaine has address 192.168.40.1
client-linux-40.mondomaine has address 192.168.40.2
ftp.mondomaine is an alias for serveur-linux-40.mondomaine.

3.6.2 : Résolution directe

host serveur-linux-40
serveur-linux-40.mondomaine has address 192.168.40.1

host client-linux-40
client-linux-40.mondomaine has address 192.168.40.2

host ftp
ftp.mondomaine is an alias for serveur-linux-40.mondomaine.
serveur-linux-40.mondomaine has address 192.168.40.1

3.6.3 : Résolution inverse

host 192.168.40.1
1.40.168.192.in-addr.arpa domain name pointer serveur-linux-40.mondomaine.

host 192.168.40.2
2.40.168.192.in-addr.arpa domain name pointer client-linux-40.mondomaine.

host 127.0.0.1
1.0.0.127.in-addr.arpa domain name pointer localhost.

III.7. Exemple de fichiers de configuration

3.7.1 : /etc/bind/named.conf.local

```
zone "mondomaine" {
        type master;
        file "/etc/bind/db.mondomaine";
};
zone "40.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.40.hosts";
};
```

3.7.2 : /etc/bind/named.conf.options

```
options {
    directory "/etc/bind";
        forwarders {
           172.17.1.1;
           172.17.2.254;
        };
};
```

3.7.3 : /etc/bind/db.mondomaine

```
$TTL 86400    ;24H
@       IN      SOA     serveur-linux-40.mondomaine. root.serveur-linux-40.mondomaine.  (
                              2022022700 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
;
@       IN      NS        serveur-linux-40.mondomaine.
serveur-linux-40        IN      A               192.168.40.1
client-linux-40         IN      A               192.168.40.2
ftp                     IN      CNAME           serveur-linux-40.mondomaine.
```

3.7.4 : /etc/bind/db.172.16.hosts

```
$TTL 86400    ;24H
@       IN      SOA     serveur-linux-40.mondomaine. root.serveur-linux-40.mondomaine.  (
                              2022022700 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
@               IN      NS      serveur-linux-40.mondomaine.
1               IN      PTR     serveur-linux-40.mondomaine.
2               IN      PTR     client-linux-40.mondomaine.
```

3.7.5 : Vérification de la configuration

On peut vérifier la syntaxe de la configuration générale du serveur DNS (fichier ***/etc/bind/named.conf***) à l'aide de la commande : **named-checkconf**.

Si la commande n'affiche aucun message d'erreur, alors il n'y a pas d'erreur de syntaxe.

On peut aussi vérifier la syntaxe du fichier de zone ***/etc/bind/db.mondomaine*** à l'aide de la commande : **named-checkzone mondomaine.org /etc/bind/db.mondomaine**.

```
named-checkzone mondomaine.org /etc/bind/db.mondomaine
zone mondomaine.org/IN: loaded serial 2022022700
OK
```

III.8. Commandes dig et nslookup

Le test du serveur **DNS** peut se faire avec des utilitaires clients communs à **Linux** et **Windows** nommés **dig** et **nslookup**. Pour disposer de ces utilitaires sous **Debian**, il faut installer le paquet **dnsutils** à l'aide de la commande **apt-get install dnsutils**.

Ces commandes peut être utilisé pour visualiser les informations d'un domaine, les types d'enregistrements etc. La commande la plus simple est **nslookup** :

```
nslookup client-linux-40.mondomaine
Server:         192.168.40.1
Address:        192.168.40.1#53
Name:           client-linux-40.mondomaine
Address: 192.168.40.2
```

Lorsque l'on saisie **nslookup** sans paramètre, on arrive sur un interpréteur de commandes sur lequel on peut ensuite effectuer des **résolutions DNS** :

```
root@debian10:~# nslookup
> client-linux-40.mondomaine
Server:         192.168.40.1
Address:        192.168.40.1#53
Name:           client-linux-40.mondomaine
Address: 192.168.40.2
```