TP2 : Résolution de nom (DNS) et configuration de service DNS

Objectifs du TP

L'objectif du TP est de comprendre les principes de fonctionnement des services de nommage DNS (Domain Name Service) et de procéder à une installation et configuration minimale de ce service. La mise en œuvre se fera à l'aide de machines virtuelles, comme en première année de BUT.

Ce TP est en plusieurs parties, organisé de la façon suivante :

— Partie 1 : découverte du service DNS

— Partie 2 : configuration et test du service DNS

1 Émettre une requête DNS

Sans que l'on s'en rende compte, les applications logicielles (par exemple, le logiciel de courrier électronique Thunderbird) permettant l'accès à un service sur le réseau (par exemple, un service d'envoi de courrier électronique SMTP) émettent des requêtes auprès d'un serveur DNS pour réaliser une résolution de nom, c'est-à-dire connaître l'adresse IP associée à un nom de machine.

Le serveur de nom auquel on s'adresse est en général celui de l'organisation (par exemple, une entreprise) ou celui indiqué par le fournisseur d'accès. Dans ce TP, le serveur de nom DNS que l'on utilise est celui de l'IUT2.

Sous Unix, il existe différents outils en ligne de commande permettant l'interrogation d'un serveur DNS : ***host***, ***nslookup***, et ***dig***. Sous Windows, la commande ***nslookup*** existe aussi.

1.1 Commande host

Dans une console, exécutez la commande :

```
host transit.iut2.univ-grenoble-alpes.fr
```

Quelle est l'adresse IP de **transit** du domaine ***iut2.univ-grenoble-alpes.fr*** ?

1.2 Commande nslookup

à partir d'un navigateur web, visualiser les deux sites web suivants :

iut2.univ-grenoble-alpes.fr

www.univ-grenoble-alpes.fr

Puis visualisez, le site web : ***ksup.u-ga.fr***

Enfin, à l'aide de la commande ***nslookup***, faire la résolution de nom pour chacun de ces trois sites web ci-dessus. Pour le premier site utilisez

```
nslookup iut2.univ-grenoble-alpes.fr 193.55.51.34
```

où **193.55.51.34** est *meije*, le serveur DNS local à l'IUT2.

A. Serveur DNS qui à répondu

1. Quelle est l'adresse IP du **serveur DNS** qui vous a répondu ?

2. Via quel numéro de port ? Est-ce conforme au protocole DNS ?
3. Quel est son nom et son domaine DNS ?

B. Réponses du serveur DNS

1. Que signifie « Non-authoritative answer » indiquée dans la réponse ? (vous pouvez consulter wikipedia)
2. Quelle est l'adresse IP de chacun des sites ?
www.univ-grenoble-alpes.fr =
iut2.univ-grenoble-alpes.fr =
ksup.u-ga.fr =
3. Pour les deux premiers sites, quelle est la valeur du champ ***canonical name*** ?
4. Que signifie l'information « Canonical Name » ?
5. Dans tous les cas, quel est le vrai nom du serveur ?
6. Que peut-on en déduire sur la relation entre de nom de machine et @IP ? Quel est l'intérêt de cette organisation ?

1.3 Commande dig (domain information groper)

La commande ***dig*** est un outil plus riche que les commandes ***host*** et ***nslookup*** : elle affiche toutes les informations contenues dans les requêtes DNS. De plus, elle offre de nombreuses options pour réaliser des requêtes DNS [1]. Utiliser la commande ***man dig*** pour obtenir des informations utiles sur cet outil.

Exécutez la commande :

```
dig +nocmd +nostats +noedns www.renater.fr.
```

puis la commande

```
dig +nocmd +nostats +noedns www.renater.fr. @g.ext.nic.fr
```

1. À quoi correspondent les sections ***QUESTION***, ***ANSWER***, ***AUTHORITY***, et ***ADDITIONAL*** ?
2. Sachant que pour la section ***ANSWER*** les informations sont présentées en colonne, qu'indique la cinquième colonne ? Notez que la plupart de ces informations sont décrites dans le cours.
3. Pour toutes les sections, dans la quatrième colonne, que signifient les sigles ***CNAME***, ***A***, ***AAAA***, et ***NS*** ?

Exécutez la commande :

```
nslookup -query=soa renater.fr.
```

4. Que signifie ***SOA*** ? Quel est le serveur primaire pour le domaine ***renater.fr*** ?

Lancer plusieurs fois la commande :

```
dig www.qwant.fr.
```

1. Une option intéressante est `+yaml` afin d'obtenir une sortie avec plus de descriptions

Et, dans la section ***ANSWER***, observer le chiffre de la seconde colonne :

1. Que constate-t-on ? Comment évolue-t-il ?

2. Que mesure ce nombre ?

2 Résolution inverse

Les commandes réalisées jusqu'à présent ont permis de retrouver l'adresse IP associée à un nom. L'objectif de cette partie est de réaliser l'opération inverse.

Exécuter la commande :

```
nslookup 195.221.57.62
```

Puis la commande :

```
dig -x 195.221.57.62
```

1. Quel est le nom associé à cette IP ?

2. Sous quelle forme la commande ***nslookup*** représente l'adresse IP donnée en paramètre ?

3. Dans la section ***ANSWER***, comment la commande ***dig*** représente l'adresse IP ?

4. A quoi correspond l'acronyme ***PTR*** ?

3 Distribution du service DNS

Cette partie vise à illustrer le caractère distribué du service DNS et comment les requêtes sont relayées entre serveurs DNS.

En effet, la particularité du service de résolution de nom est qu'il est distribué : il n'existe pas une base de données unique mais plusieurs "morceaux" répartis sur plusieurs DNS, en domaines et sous-domaines.

Ces domaines sont organisés pour former un arbre : à chaque nœud correspond un ou plusieurs serveurs DNS. Ainsi, le serveur ***meije*** couvre uniquement le domaine ***iut2.univ-grenoble-alpes.fr.***

Par conséquent, lorsqu'une machine du domaine ***iut2.univ-grenoble-alpes.fr*** requiert la résolution de nom pour un domaine différent, par exemple ***kernel.org***, celle-ci est relayée indirectement au serveur DNS correspondant.

3.1 Serveurs DNS du domaine iut2.univ-grenoble-alpes.fr.

Exécuter la commande :

```
dig iut2.univ-grenoble-alpes.fr. ns
```

L'option ***ns*** permet de lister l'ensemble des serveurs DNS pour un domaine.

Donner deux exemples de serveurs DNS (section ***ANSWER***) couvrant le domaine ***iut2.univ-grenoble-alpes.fr.***

3.2 Serveurs DNS du domaine univ-grenoble-alpes.fr.

Exécuter la commande :

```
dig univ-grenoble-alpes.fr. ns
```

1. Donner deux exemples de serveurs DNS (section ***ANSWER***) couvrant le domaine ***univ-grenoble-alpes.fr.***

2. Ces serveurs sont-ils dans le même réseau ? Si ce n'est pas le cas, pourquoi est-ce alors possible ?

3.3 Serveurs DNS du domaine racine et de 1er niveau (TLD)

Exécuter la commande :

```
dig fr. ns
```

Puis :

```
dig . ns
```

1. À quoi correspondent les 4 dernières commandes que vous venez d'effectuer (parties 3.1, 3.2 et 3.3) ?
2. Que représente le "." pour la dernière commande ?
3. Combien existe-t-il de serveurs DNS pour le domaine racine d'après la dernière commande ?
4. Quelle est la particularité de leur nom ?
5. Dessiner un arbre avec le "." à la racine, avec les branches ***.fr.*** et ***.org.*** et les exemples des commandes précédentes. Indiquer le nom d'un serveur DNS pour chaque nœud de votre arbre.

6. Compléter l'arbre pour les domaines ***kernel.org.***, ***laposte.fr.***, ***univ-grenoble-alpes.fr.***

3.4 Serveurs DNS et résolution inverse : arbre de résolution inverse

Exécuter les commandes suivantes :

```
dig 57.221.195.in-addr.arpa. ns
```

```
dig 221.195.in-addr.arpa. ns
```

```
dig 195.in-addr.arpa. ns
```

```
dig in-addr.arpa. ns
```

```
dig arpa. ns
```

1. Donner le nom et l'adresse IP d'un des serveurs DNS couvrant le domaine ***57.221.195.in-addr.arpa.*** Donner également un exemple de serveur DNS pour les autres requêtes.

2. Compléter l'arbre de la question 3.3 avec les différents domaines.

4 Résolution itérative d'une requête DNS

Exécuter la commande :

```
dig +trace +nodnssec www.qwant.fr
```

L'option ***+trace*** permet de visualiser quels sont les domaines interrogés par un serveur DNS quand il en a besoin.

1. De quel domaine est le premier serveur DNS interrogé par le serveur DNS de l'IUT2 ? Est-ce logique ? Pourquoi ?

2. Quels sont les différents serveurs DNS qui ont répondu ?

3. Qu'en déduire sur le mécanisme utilisé pour relayer des requêtes DNS ? Faire un schéma montrant la suite des appels depuis l'envoi de la requête DNS jusqu'à la réponse reçue par le client.

5 Schéma de base de données d'un serveur DNS

Pour réaliser une base de données, si vous aviez à modéliser (ex. avec UML) les relations existant entre adresses IP et noms de machine enregistrés dans le DNS, quelle serait leur cardinalité (cf. cardinalité wikipedia) ?

6 DNS menteur

Le contrôle des serveurs DNS est un élément essentiel de la mise en place de décisions de justice ou de contrôle de l'espace internet national. Les décisions nationales n'impactent souvent que les DNS nationaux voire uniquement ceux des FAI les plus importants.

Un exemple est le site de *The Pirate Bay* qui après plusieurs années d'action en justice s'est vu confirmer la légalité de son blocage en Europe par la Cour de justice de l'Union européenne en 2017. Selon les pays, ce blocage est mis en œuvre à travers une manipulation de l'espace des noms de domaine (*DNS hijacking* ou *DNS Mangling*). On appelle DNS menteurs les serveurs DNS qui mettent en place une telle manipulation.

Dans le fonctionnement normal des DNS, lorsqu'un domaine ou un sous-domaine n'existe pas ou est inaccessible le serveur doit vous renvoyer un code d'erreur indiquant que le domaine est introuvable (**NXDOMAIN**, « ce domaine n'existe pas »). Les DNS menteurs, vont soit prétendre

qu'un nom de domaine existant n'est pas accessible, soit amener l'utilisateur vers une autre destination. Dans le second cas, ces systèmes sont souvent mis en place pour pouvoir placer des liens publicitaires sur les pages d'erreur.

1. En utilisant un serveur DNS d'orange (194.2.0.20 ou 194.2.0.50) faites une requête nslookup sur
www.univ-grenoble-alpes.fr
www.kernel.org
sci-hub.se
que vous renvoie ces trois requêtes ?
2. Refaite les requêtes en utilisant le serveur 1.1.1.1 de l'entreprise américaine Cloudflare
Quelle(s) différence(s) constatez-vous ?
3. Qu'en concluez-vous sur le premier serveur DNS ? Vérifier en fonction de l'article Sci-Hub si le comportement de ces deux serveurs est logique.

7 Configuration d'un serveur DNS

Dans cette partie, vous travaillerez uniquement avec la VM Serveur.

7.1 Étude de la configuration par défaut et des différents fichiers

Le répertoire `/etc/bind` contient la configuration de l'outil `bind9`, capable de mettre en œuvre un service DNS.

Le fichier `named.conf.default-zones` est le fichier de configuration principal. Son contenu indique comment lui sont rattachés les autres fichiers. En déduire un schéma montrant les dépendances entre ces fichiers (option file) :

Par déduction, que configurent les fichiers suivants ?

Fichier	Type de configuration
/etc/bind/db.root	
/etc/bind/db.local	
/etc/bind/db.127	

7.2 Syntaxe des entrées de la base de noms du DNS

Par défaut, le domaine `jaune.fr` est déclaré. Les déclarations de ce domaine sont dans le fichier `db.jaune.fr`

La syntaxe générale des entrées est la suivante avec des variations pour le champ `[valeur]` selon le type d'entrées :

`[clé] IN [type d'entrée] [valeur]`

Pour chaque type d'entrées, pour le domaine jaune.fr, la syntaxe est la suivante :

Type SOA (Start Of Authority) : identifie le serveur primaire de la zone (le @ identifie le nom de domaine courant pour la zone couverte par le fichier)

```
@ IN SOA [nom d'hôte complet]. root.[nom de domaine complet]. ([Serial] [Refresh] [Retry] [Expire] [TTL])
; par exemple
@ IN SOA fruits.jaune.fr. root.jaune.fr. (20180910 3600 600 84600 600)
```

Type NS (Name Server) : identifie un des serveurs DNS (dont le SOA) pour la zone par une association (nom de domaine, nom d'hôte complet)

```
@ IN NS [nom d'hôte complet].
; par exemple
@ IN NS fruits.jaune.fr.
```

Type A : résolution de noms = association (nom d'hôte, adresse IP)

```
[nom d'hôte] IN A [adresse IP]
; par exemple
banane IN A 11.22.33.99
```

Type PTR : résolution inverse = association (numéro de machine, nom d'hôte complet)

```
[numéro d'hôte] IN PTR [nom d'hôte complet].
; par exemple
99 IN PTR banane.jaune.fr.
```

Type CNAME : résolution d'alias = association (nom d'hôte, nom d'hôte complet)

```
[nom d'hôte] IN CNAME [nom d'hôte complet].
; par exemple
poire IN CNAME banane.jaune.fr.
```

7.3 Tester le service DNS pour le domaine jaune.fr

Au préalable, vérifiez que le fichier `/etc/resolv.conf` contient la ligne suivante (le créer/modifier si besoin) :

`nameserver 11.22.33.1`

Démarrez le service DNS :

```
systemctl start bind9
```

Faites les requêtes DNS suivantes :

```
nslookup fruits.jaune.fr
```

```
nslookup banane.jaune.fr
```

Arrêtez le service DNS :

```
systemctl stop bind9
```

7.4 Configurer le service DNS pour le domaine rouge.fr

Le fichier `/etc/bind/db.rouge.fr` contient les entrées pour la résolution des noms associés au domaine rouge.fr, d'adresse réseau `77.88.99.0/24`. À l'aide d'un éditeur de texte, modifiez et complétez ce fichier de telle sorte que l'on y trouve les entrées suivantes (voir tableau ci-dessous) : A et CNAME.

Clé	Type d'entrée	Valeur
fruits	A	`77.88.99.64`
framboise	A	`77.88.99.47`
fraise	A	`77.88.99.16`
groseille	CNAME	fruits.rouge.fr.

Modifiez les paramètres de telle sorte que la durée de vie (TTL) des entrées soit réglée à 20 minutes. Pour vérifier les erreurs de syntaxe, utilisez la commande :

```
named-checkzone -t /etc/bind rouge.fr db.rouge.fr
```

Une fois ces configurations réalisées, lancer le service DNS :

```
systemctl start bind9
```

ATTENTION : Si vous modifiez les fichiers de configuration une fois le service bind9 démarré, il faut penser à l'arrêter puis à le redémarrer pour prendre en compte les modifications.

Puis, avec la commande `host`, `nslookup` ou `dig`, testez la résolution des noms suivants : `fruits.rouge.fr`, `framboise.rouge.fr`, `fraise.rouge.fr`, et `groseille.rouge.fr`.

7.5 Configurer le service DNS pour la résolution inverse

Le fichier `/etc/bind/db.77.88.99` contient les entrées pour la résolution inverse des noms associés au domaine `rouge.fr`. Créez et éditez ce fichier pour qu'il contienne :

1. Des entrées SOA et NS similaire au fichier `/etc/bind/db.11.22.33`
2. Une entrée de type PTR pour chaque entrée `A` du fichier `/etc/bind/db.rouge.fr` correspondante.

Le numéro de machine correspond à la partie de son adresse IP sans la portion correspondant à l'adresse réseau (ici `77.88.99/24`). Dans notre exemple (réseau /24), ce numéro est donc le quatrième nombre de l'adresse IP.

Pour vérifier les erreurs de syntaxe, utiliser la commande :

```
named-checkzone -t /etc/bind 99.88.77.in-addr.arpa db.77.88.99
```

Relancez le service bind9 et tester :

```
nslookup 77.88.99.64
```

```
nslookup 77.88.99.16
```

```
nslookup 77.88.99.100
```

7.6 Déclarer le domaine vert.fr

Le fichier named.conf.default-zones est le fichier de configuration permettant de déclarer les zones couvertes par le service DNS. Il s'agit de simplement déclarer un nouveau domaine, vert.fr (les entrées de ce domaine sont déjà saisies).

En vous inspirant des zones « jaunes.fr » et « 33.22.11.in-addr.arpa », éditez ce fichier (**partie notée //// À COMPLETER ////**) pour ajouter deux nouvelles zones :

— La zone `vert.fr` pour la résolution de noms sur le domaine `vert.fr`.

— la zone `66.55.44.in-addr.arpa` pour la résolution inverse correspondante

Pour vérifier les erreurs de syntaxe, utilisez la commande :

```
named-checkconf -t /etc/bind named.conf.default-zones
```

Relancez le service bind9 et testez :

```
nslookup citron.vert.fr
```

```
nslookup 44.55.66.231
```

8 Vérification de fonctionnement du service DNS depuis le client (VM Client)

Refaites les tests (*nslookup*) des parties 7.3, 7.4 et 7.5 depuis la VM client.