SCR.1.2 TP 15 ⊥ :

Le système DNS

RFCs 1034 et 1035

`dig` - `nslookup` - `host`

I. Introduction et rappel du cours.

Dans le contexte DNS, l'*espace de noms de domaines* désigne un ensemble d'objets appelés ressources. L'espace est structuré en une arborescence dont les feuilles sont typiquement des machines. Le sous-arbre associé à un nœd de l'arbre correspond à un sous-ensemble de ressources.

Chaque nœud a un *label*. Le label chaîne vide est réservé à la racine. Le nom de domaine d'un nœud est la liste des labels des nœuds se trouvant sur le chemin de l'arborescence entre le nœud en question et la racine (comprise). Par convention, cette liste lorsque lue de la gauche vers la droite, associe les labels en partant du nœud en question et en remontant vers la racine. L'utilisateur soumet ces noms aux programmes pertinents en séparant les labels de la liste par le symbole . (period).

Exemple : `xx.lcs.mit.edu.`

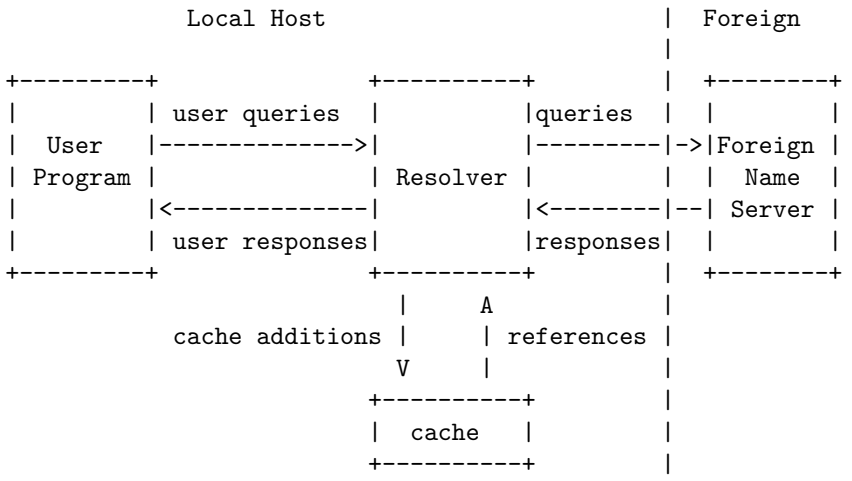
Les noms de domaine fournissent un mécanisme pour nommer les ressources de telle sorte que les noms soient compatibles pour une utilisation dans différents hosts, familles de protocoles, organisations administratives, internet.

Les applications réseaux font des requêtes à un agent local (une fonction dans le noyau) appelé *resolver* qui retrouve les informations relatives à l'espace de nommage en questionnant des serveurs de noms.

— Les requêtes vers le *resolver* sont faites à travers des appels système. Par exemple, le code de la commande `ping` sollicite le *resolver* pour obtenir l'adresse correspondant à l'argument passé à `ping`.

— Du point de vue de l'utilisateur, les noms de domaine sont utiles comme arguments aux *resolvers*.

— Du point de vue du *resolver*, la base de données qui constitue l'espace de nommage est distribuée sur différents serveurs de noms.



— Les serveurs de noms gèrent deux sortes de données. La première sorte de données constituent des sous-ensembles appelés *zones*. Chaque zone est la base de données complète d'un sous-arbre (éventuellement "amputé" par endroits) de l'espace de nommage. Ces données sont dites *authoritative*, c'est à dire faisant autorité. Un serveur de noms vérifie périodiquement que ses zones sont à jour. Le cas échéant, il obtient une copie récente des zones mises à jour à partir de fichiers maîtres (*master files*) stockés localement ou

dans un autre serveur. La seconde sorte de données sont des données en cache obtenue précédemment par un *resolver* local. Ces données peuvent être incomplètes mais elles améliorent les performances du processus de résolution lorsqu'on doit avoir accès de manière répétée aux mêmes données non locales. Les données en cache finissent par disparaître par un mécanisme d'expiration de temps *timeout*.

1. Quel fichier consulter pour trouver l'adresse IP du serveur de noms interrogé par défaut par un *resolver* local ?
2. À l'aide d'une des commandes qui implémentent un client vers un serveur de noms, trouver le nom de la machine précédente.

II. L'en-tête du message *domain* - RFC 1035 -

On va passer deux lignes de commandes interrogeant le serveur de noms par défaut sur le nom `iluvatar.arda.lan` puis sur le nom `arda.com.` Dans chacun des cas, on tracera le traffic d'abord par `tshark` puis par `tcpdump` en recueillant, à chaque fois, le résultat dans un fichier séparé.

1. Préparer une ligne de commande `tshark` en filtrant par les options et l'expression afin de n'avoir que l'affichage relatif à l'échange dns que l'on s'apprête à provoquer.
2. Lancer une commande `dig` interrogeant sur le nom `iluvatar.arda.lan` sans préciser le type désiré pour les ressources.
3. Le serveur a répondu sur un seul type de ressource pour le nom `iluvatar.arda.lan`. Lequel ?
4. Dans l'affichage fourni par `dig`, des informations sont placées dans la section *header*. En analysant la trace fournie par `tshark` retrouver la signification de ces informations.
5. Dans l'affichage fourni par `dig`, comment le serveur précise-t-il s'il est ou non une autorité sur le nom de domaine soumis dans la question ? Qu'en est-il dans le cas présent ?
6. Le serveur a communiqué un temps de vie pour la ressource. De combien ? À quoi sert-il ?
7. Retrouver les mêmes informations dans une trace fournie par `tcpdump`.
8. Refaire 1, 2 et 5 en interrogeant cette fois-ci sur le nom `arda.com`. En comparant au `dig` précédent, quelle différence dans les informations placées dans la section *header* de la réponse à `dig` ?

III. RRs mis en cache et TTLs.

1. Réaliser un `dig` sur `vintage.com` et noter le TTL fourni dans la section réponse. Refaire le même `dig`. Qu'onserve-t-on quant à la valeur du TTL pour le même RR ? Expliquer.
2. Refaire 1 avec cette fois-ci un `dig` sur `iluvatar.arda.lan`. Quelle différence note-t-on quant aux valeurs TTL suite à plusieurs lancements de la même commande `dig` ? Expliquer ?
3. A-t-on la possibilité de décider d'utiliser une donnée qui ne provient pas du cache ? Si oui, indiquer comment faire ? Sinon, expliquer quelle spécification DNS l'interdit.