LABO4 - DNS

1 OBJECTIFS

Découvrir le service DNS (Domain Name System)

2 RAPPELS

2.1. FQDN (Fully qualified domain name)

On entend par FQDN (Fully qualified domain name) ou Nom de domaine pleinement qualifié un nom de domaine écrit de façon absolue, y compris tous les domaines jusqu'au domaine de premier niveau (TLD), il est ponctué par un point final. Dans une réseau TCP/IP, une adresse FQDN sera l'association entre le nom de la machine et le domaine auquel elle appartient.

2.2. Notions de résolution

2.2.1 Résolution de noms directe

Dans un réseau IP, lorsqu'une machine A veut communiquer avec une machine B, la machine A connaît le nom FQDN de B.

Pour que A puisse communiquer avec B grâce au protocole IP, A va avoir besoin de connaître l'adresse IP de B.

A doit posséder un moyen d'effectuer la résolution de noms directe, c'est-àdire un moyen de trouver l'adresse IP de B à partir de son nom qualifié.

Le ***résolveur*** est le programme chargé de cette opération.

2.2.2 Résolution de noms inverse

La machine B reçoit un datagramme IP en provenance de A. Ce datagramme contient l'adresse IP de A. B peut avoir besoin de connaître le nom FQDN de la machine A.

B doit donc être capable de trouver le nom FQDN de A à partir de son adresse IP. C'est ce qu'on appelle la résolution de noms inverse.

Le ***résolveur*** est également chargé de cette opération.

Remarque : La déclaration inverse est importante sur les adresses IP publiques Internet puisque l'absence d'une résolution inverse est considérée comme une erreur opérationnelle (RFC 1912) qui peut entraîner le refus d'accès à un service. Par exemple, un serveur de messagerie électronique se présentant en envoi avec une adresse IP n'ayant pas de résolution inverse a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier (message de refus de type : IP lookup failed).

3 RESOLVER SOUS LINUX

3.1. Résolution de noms par fichier hosts

Le fichier **/etc/hosts** comprend l'adresse FQDN de chaque machine du réseau ainsi que son adresse IP.

3.2. Résolution de nom par serveur DNS

On installe un serveur de noms sur le réseau. Chaque machine du réseau doit connaître l'adresse IP de ce serveur DNS. Dès qu'une machine veut effectuer une résolution de noms directe ou inverse, elle va interroger le serveur de noms. L'administrateur doit configurer le serveur de noms pour que ce dernier connaisse l'adresse IP et le nom de toutes les machines du réseau.

3.3. Configuration de la résolution de noms

Le fichier **/etc/host.conf** contient des informations spécifiques pour la configuration de la bibliothèque de résolution de noms.

Le mot-clé **order** indique dans quel ordre la résolution des noms d'hôtes doit avoir lieu. Il doit être suivi par une ou plusieurs méthodes séparées par des virgules. Ces méthodes sont (généralement dans cet ordre) : **hosts**, **bind**. Ce qui correspond à faire d'abord une résolution locale par le fichier **hosts**, puis par un accès à un serveur DNS (**bind**).

Pour en savoir plus, faire : **man host.conf**

3.4. Fichier de configuration de la résolution de noms

Le fichier **/etc/resolv.conf** contient des informations utilisées par le ***resolver*** pour accéder au système DNS Internet.

Les options de configuration de base sont :

- **nameserver** adresse IP du serveur de noms que le ***resolver*** interrogera
- **search** Nom du domaine local

Pour en savoir plus, faire : **man resolv.conf**

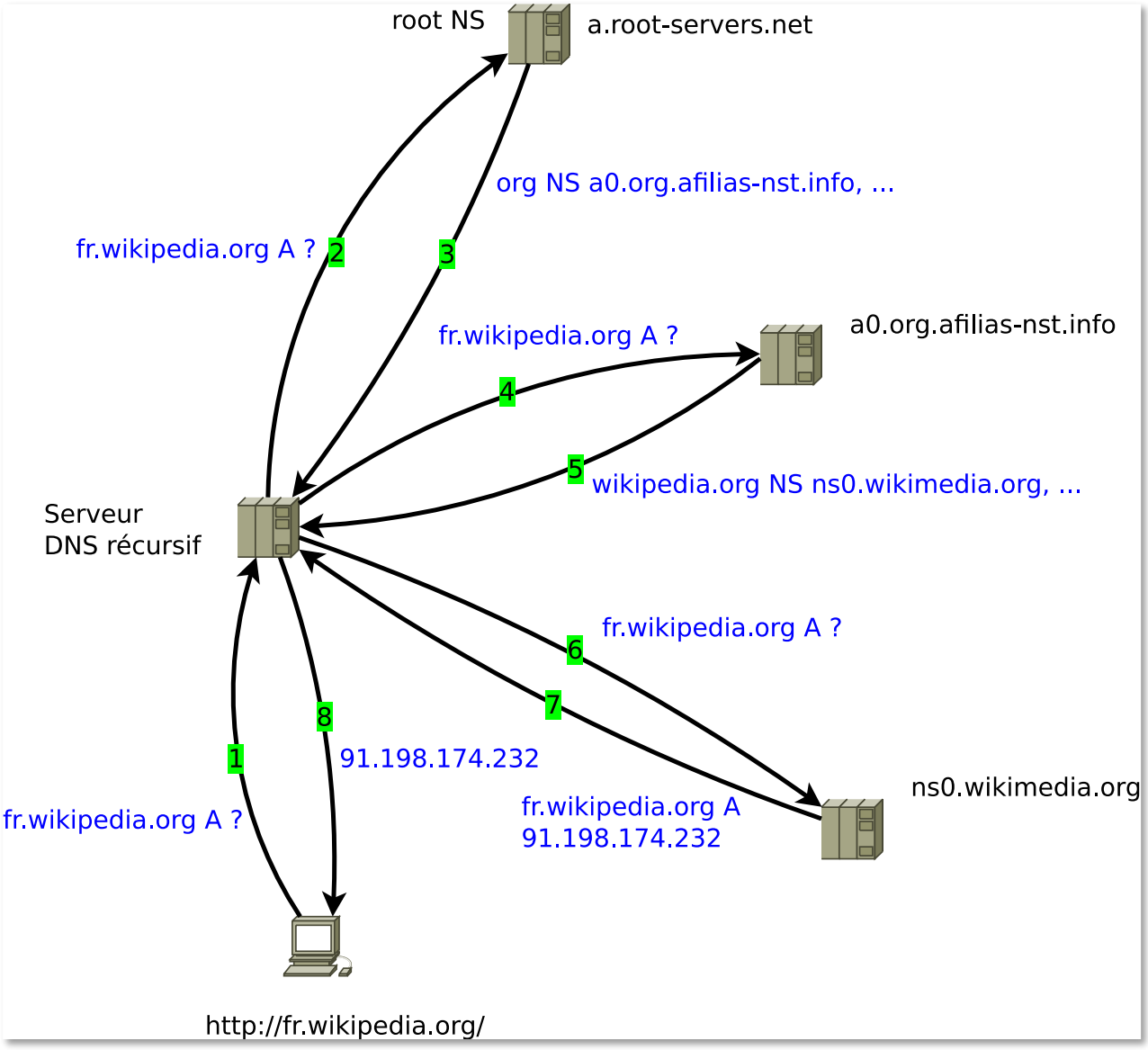
4 EXERCICES 1

1. Que contient votre fichier /etc/hosts ?
   `cat /etc/hosts`
2. Dans quel ordre se fera la résolution de noms sur votre machine ?
   `cat /etc/host.conf`
3. Quelles sont les adresses IP du serveur de noms DNS que le résolveur interrogera ?
   `cat /etc/resolv.conf`

5 TYPES DE REPONSES DNS

Quand un système doit résoudre un nom, ils s'adressent à un ou plusieurs serveurs DNS dits récursifs, c'est-à-dire qui vont parcourir la hiérarchie DNS et faire suivre la requête à un ou plusieurs autres serveurs DNS pour fournir une réponse. Les fournisseurs d'accès à Internet mettent à disposition de leurs clients ces serveurs récursifs.

Quand un serveur DNS récursif doit trouver l'adresse IP de **fr.wikipedia.org**, un processus itératif démarre pour consulter la hiérarchie DNS. Le serveur DNS récursif demande aux serveurs DNS appelés serveurs racine quels serveurs peuvent lui répondre pour la zone org. Parmi ceux-ci, notre serveur va en choisir un pour savoir quels serveurs sont capables de lui répondre pour la zone wikipedia.org. C'est un de ces derniers qui pourra lui donner l'adresse IP de fr.wikipedia.org. S'il se trouve qu'un serveur ne répond pas, un autre serveur de la liste sera consulté.



Pour optimiser les requêtes ultérieures, les serveurs DNS récursifs font aussi office de DNS cache : ils gardent en mémoire (cache) la réponse d'une résolution de nom afin de ne pas

effectuer ce processus à nouveau ultérieurement. Cette information est conservée pendant une période nommée **Time to live** et associée à chaque nom de domaine.

Un nom de domaine peut utiliser plusieurs serveurs DNS. Généralement, les noms de domaines en utilisent au moins deux : un primaire et un secondaire. Il peut y avoir plusieurs serveurs secondaires.

L'ensemble des serveurs primaires et secondaires font autorité pour un domaine, c'est-à-dire que la réponse ne fait pas appel à un autre serveur ou à un cache. Les serveurs récursifs fournissent des réponses qui ne sont pas nécessairement à jour, à cause du cache mis en place. On parle alors de réponse ne faisant pas autorité (**non-authoritative answer**).

Cette architecture garantit au réseau Internet une certaine continuité dans la résolution des noms. Quand un serveur DNS tombe en panne, le bon fonctionnement de la résolution de nom n'est pas remis en cause dans la mesure où des serveurs secondaires sont disponibles.

5.1. La commande dig

La commande **`dig`** sous Linux est plus complète. Dig a l'avantage (ou l'inconvénient) de présenter les informations sous une forme directement utilisable dans un fichier de configuration de Zone DNS.

Suite à une commande dig, les flags renvoyés, lorsqu'ils sont présents, ont la signification suivante :

- qr (query response) indique qu'il s'agit d'une réponse à une requête.
- aa (authoritative answer) indique que la réponse vient directement d'un serveur faisant autorité.
- rd (recursion desired) indique qu'une requête récursive est demandée (par défaut).
- ra (recursion available) indique que la récursivité est disponible.

La commande **`host`** permet elle aussi de chercher des noms de machine à l'aide d'un serveur de domaine.

6 EXERCICE 2

4. Déterminez l'adresse de **www.helmo.be**
   ```
   host www.helmo.be
   host -v www.helmo.be
   ```

Remarque : les enregistrements de type A (address) se trouvent dans la zone directe et permettent l'associer une adresse FQDN à une adresse IP. En général, chaque machine possède un enregistrement de type A dans sa zone directe.

5. Déterminez si la réponse du serveur DNS qui vous a répondu supporte la récursivité et si sa réponse fait autorité (« authoritative »).
   ```
   dig www.helmo.be
   ```

Remarque : les enregistrements NS (name server) permettent de spécifier les serveurs de noms ayant autorité sur le domaine. Chaque fichier de zone comporte en général un tel enregistrement. Dans la zone be, les record NS suivants créent le sous-domaine helmo et délèguent celui¬ci vers les serveurs indiqués. L'ordre des serveurs est quelconque. Tous les serveurs indiqués doivent faire autorité pour le domaine.

6. Déterminez le serveur à utiliser pour obtenir une réponse « **authoritative** ». Ce serveur supporte-t-il la récursivité ?
   ```
   host -v -t ns helmo.be
   ```
   ….
   Remplacez par un <serveur_DNS>
   ```
   dig @<serveur_DNS> www.helmo.be
   ```

7. Quelle réponse vous donne un serveur DNS lorsqu'il ne supporte pas la récursivité et qu'il ne connaît pas la réponse à votre question ?
   Vous pouvez par exemple utiliser un serveur de nom d'un domaine pour résoudre le nom d'un autre domaine de même niveau :
   ```
   dig @ns1.google.com www.yahoo.fr
   ```

8. Visualisez, avec l'option **+trace** la suite des serveurs DNS contactés pour trouver l'adresse IP de www.helmo.be.
   ```
   dig +trace www.helmo.be
   ```

9. Quels sont les domaines traversés et les serveurs de noms interrogés ? La requête est-elle récursive ?

10. Recherchez plusieurs fois l'adresse www.lasalle84.org. Que remarquez-vous ?

11. Qui est en charge de la zone **be** ?
    ```
    dig ns @a.rootservers.net. be
    ```

*Remarque : Il existe 13 serveurs racine, nommés de **a** à **m**.root-servers.net (http://www.rootservers.org/). Ces serveurs sont gérés par douze organisations différentes : deux sont européennes, une japonaise et les neuf autres sont américaines.*

12. Quelles sont les informations contenues dans les entrées de type **SOA** du DNS ?
    ```
    host -v -a helmo.be ns.helmo.be
    dig soa @ns.helmo.be helmo.be +multiline
    ```

Remarque : les enregistrements SOA (Start Of Authority) donnent les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone. Il désigne l'autorité (start of authority) ou le responsable de la zone dans la hiérarchie DNS.
Cet enregistrement permet d'indiquer le serveur de nom maître (primaire), l'adresse e-mail d'un contact technique (avec @ remplacé par un point) et des paramètres d'expiration. Ces paramètres sont dans l'ordre :

- *Serial : indique un numéro de version pour la zone. Ce nombre doit être incrémenté à chaque modification du fichier zone ; on utilise par convention une date au format «yyyymmddhhmm » (« yyyy » pour l'année sur 4 chiffres, « mm » pour le mois sur 2 chiffres, « dd » pour le jour sur 2 chiffres, « hh » pour l'heure sur 2 chiffres et « mm » pour les minutes sur 2 chiffres) ;*
- *Refresh : l'écart en secondes entre les demandes successives de mise à jour réalisées depuis le serveur secondaire ou les serveurs esclaves ;*
- *Retry : le délai en secondes que doivent attendre le serveur secondaire ou les serveurs esclaves lorsque leur précédente requête a échoué ;*
- *Expire : le délai en secondes au terme duquel la zone est considérée comme invalide si le secondaire ou les esclaves ne peuvent joindre le serveur primaire ;*
- *Minimum ou negative TTL : utilisé pour spécifier, en secondes, la durée de vie pendant laquelle sont conservées en cache les réponses qui correspondent à des demandes d'enregistrements inexistants*

13. Comment déterminer la durée de validité d'une adresse **A** ?

Remarque : Chaque enregistrement est associé à un Time to live (TTL) qui détermine combien de temps il peut être conservé dans un serveur cache. Ce temps est typiquement d'un jour (86400 s) mais peut être plus élevé pour des informations qui changent rarement, comme des records NS. Il est également possible d'indiquer que des informations ne doivent pas être mises en cache en spécifiant un TTL de zéro. Certaines applications, comme des navigateurs web disposent également d'un cache DNS, mais qui ne respecte pas nécessairement le TTL du DNS.

14. Quelle est la durée de vie de l'adresse **www.dyndns.org** et celle de **station-stchamas.dyndns.org** ?
    Consultez la page http://fr.wikipedia.org/wiki/DynDNS

15. Effectuez plusieurs requêtes successivement. Que remarquez-vous ?

16. Déterminez le nom de la machine d'adresse **192.0.32.7** et le serveur de noms qui gère cette résolution inverse.
    `dig -x 192.0.32.7`

Remarque : À l'inverse d'une entrée de type A, une entrée PTR indique à quel nom d'hôte correspond une adresse IPv4. Si elle est spécifiée, elle doit contenir l'enregistrement inverse d'une entrée DNS A.

17. www.yahoo.fr est-il un nom canonique ou un alias ?

Remarque : un enregistrement CNAME (canonical name record) permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original.

18. Déterminez le ou les serveur(s) d'échange de courrier pour le domaine helmo.be.
    `dig mx helmo.be`

Remarque : Une entrée DNS MX indique les serveurs SMTP à contacter pour envoyer un courriel à un utilisateur d'un domaine donné.