Administration réseau
Master IDL - parcours GLIA
Année universitaire 2009-2010

Familiarisation avec le DNS

Le but de ce TP est de se familiariser avec le DNS par l'intermédiaire de l'outil `dig`.

Utilisation : l'outil `dig` a deux utilisations principales :
- Un outil de gestion du DNS.
- Un outil de test de mise en œuvre de DNS.

Consigne : le TP doit être réalisé sous Linux.

1 Rappels

- La chaîne `IN` signifie Internet.
- La chaîne `A` signifie « adresse IPv4 », la chaîne `AAAA` signifie « adresse IPv6 ».
- La chaîne `NS` signifie « serveur de noms ».
- La chaîne `SOA` donne le nom du serveur de noms responsable.
- La chaîne `MX` indique un nom de serveur de email SMTP.
- La chaîne `TXT` indique un champ textuel.

2 Interrogation du domaine racine

Lancez la commande `dig` sans paramètre.

Exercice 1. Localisez dans la réponse de la commande l'adresse IP du serveur DNS interrogé. Localisez aussi le port utilisé par DNS. Quel est le fichier de configuration qui contient l'adresse du serveur de noms (aidez-vous de la page de manuel de `dig`) ?

2.1 Section « requête »

Exercice 2. Localisez la requête formulée par `dig`. Elle se trouve dans la section « requête ». Quel est le nom du domaine recherché ?

2.2 Section « réponse »

Exercice 3. En regardant dans la section « réponse », déterminez le nombre de réponses à la requête précédente. Validez cette réponse en cherchant sur Internet le nombre de serveurs racines.

Exercice 4. Lancez deux fois à la suite la commande `dig` sans paramètre et observez l'ordre des réponses. Est-ce que l'ordre des réponses est le même ? Si non, comment varie-t'il ?

Exercice 5. Est-ce que la section « réponse » contient des adresses IP ? Peut-on pinger le domaine racine ?

2.3 Section « additionnelle »

Exercice 6. Quelles informations trouve-t'on dans la section additionnelle ? Est-ce que ces informations sont complètes ? Pourquoi ?

Exercice 7. Peut-on pinger un routeur racine (comme le routeur `A` par exemple) ?

Exercice 8. Pourquoi peut-on pinger un routeur racine mais pas le domaine racine ?

3 Interrogation récursive concernant `univ-bpclermont.fr.`

Lancez la commande `dig univ-bpclermont.fr.` (sans oublier le point final qui qualifie un nom de domaine complet).

Exercice 9. Avez-vous obtenu une adresse IP pour `univ-bpclermont.fr.` ?

Un champ `SOA` (pour *start of autority*) indique dans l'ordre : un serveur de noms faisant autorité pour la zone donnée, un serveur de contact, la date de modification du fichier de zone et des intervalles concernant les mises à jour entre le serveur maître et ses serveurs esclaves.

Exercice 10. Quel est le nom du serveur de noms responsable de `univ-bpclermont.fr` ?

Exercice 11. Exécutez la commande `dig` sur le serveur de noms responsable de `univ-bpclermont.fr`. Quelle est l'adresse IP de ce serveur ?

Exercice 12. Quels sont les serveurs DNS qui ont autorité sur `univ-bpclermont.fr` ? Pourquoi trouve-t'on le serveur `ns2.nic.fr` ?

3.1 Adresses IPv6

Exercice 13. Est-ce que le serveur de noms responsable du domaine `univ-bpclermont.fr` a une adresse IPv6 ?

Exercice 14. En interrogeant le serveur de noms responsable de `univ-bpclermont.fr`, pouvez-vous fournir l'adresse IPv6 du serveur `ns2.nic.fr` ?

Exercice 15. En interrogeant directement `ns2.nic.fr`, obtenez-vous son adresse IPv6 ?

3.2 Renseignements complémentaires

Exercice 16. Demandez l'obtention de renseignements complémentaires sur `ns2.nic.fr` en utilisant la commande `dig ns2.nic.fr any`. Quels informations supplémentaires obtenez-vous ? Vérifiez bien la section « réponse ».

Exercice 17. Demandez des informations supplémentaires sur `univ-bpclermont.fr.`. À quoi correspond le champ MX ?

Exercice 18. Si un email est envoyé à l'utilisateur `lambda@univ-bpclermont.fr`, sur quelle serveur SMTP faudra-t'il se connecter pour que le message parvienne à l'utilisateur ? Vérifiez que le port SMTP est ouvert sur cette machine en utilisant un `telnet`[1].

Exercice 19. Est-ce qu'il est possible d'envoyer un email à un utilisateur `nom@google.fr` ?

Exercice 20. Est-ce qu'il est possible d'envoyer un email à un utilisateur `nom@gmail.com` ?

Exercice 21. Combien de noms de serveurs mails correspondent à `gmail.com` ?

3.3 Serveur HTTP

Exercice 22. Obtenez l'adresse des serveurs `www.univ-bpclermont.fr` et `www.google.com`. Vérifiez que ces adresses sont bonnes en pingant chacun de ces serveurs (par leur nom).

Exercice 23. En obtenant les informations sur ces serveurs, vous voyez apparaître un champ `CNAME`. À quoi sert ce champ ?

Exercice 24. Est-ce que `google.com` correspond à une machine ? Combien d'adresses IP correspondent à cette machine ?

Exercice 25. Est-ce que `univ-bpclermont.fr` correspond à une machine ?

Exercice 26. Qu'est-ce que la différence entre `google.com` et `univ-bpclermont.fr` implique pour un utilisateur *lambda* ?

4 Interrogation non récursive de `www.univ-bpclermont.fr.`

À présent, nous allons interroger les serveurs DNS de manière non récursive. Pour cela, nous utiliserons la syntaxe suivante : `dig @server lirep.univ-bpclermont.fr. +norecurse`, où `server` est le nom du serveur DNS questionné.

Exercice 27. Récupérez l'adresse IP d'un serveur racine (par exemple le serveur `A.ROOT-SERVERS.NET.`).

Exercice 28. Demandez à `A.ROOT-SERVERS.NET.` les serveurs ayant autorité sur `lirep.univ-bpclermont.fr.`. Localisez l'adresse IP du serveur `A.NIC.fr.`.

Exercice 29. Demandez à `A.NIC.fr.` les serveurs ayant autorité sur `lirep.univ-bpclermont.fr.`. Localisez l'adresse IP du serveur `ubpdns.univ-bpclermont.fr.`.

Exercice 30. Demandez à `ubpdns.univ-bpclermont.fr.` l'adresse IP de `lirep.univ-bpclermont.fr.`.

Exercice 31. Obtenez toutes les informations sur `sancy.univ-bpclermont.fr.`.

Exercice 32. Obtenez toutes les informations sur `lirep.univ-bpclermont.fr.`.

[1] Pour quitter une session `telnet` connectée, il faut taper `Ctrl` et le caractère] (éventuellement suivi de `Enter`), puis taper `quit`.

5 Domaines inexistants

Exercice 33. Comment pouvez-vous identifier que le domaine `bonjour.` n'existe pas ?

6 Résolution inverse non récursive

Pour obtenir le nom d'une machine à partir de son adresse IP, il faut utiliser la commande suivante : `dig @server d.c.b.a.in-addr.arpa +norecurse any` de manière itérative, où `a.b.c.d` est l'adresse IP de la machine et `server` est le nom du serveur interrogé.

Exercice 34. Obtenez le nom de la machine dont l'adresse est `a.b.c.d` en faisant une résolution inverse non récursive à partir d'un serveur racine. Représentez graphiquement la suite de serveurs que vous interrogez.

Exercice 35. Que signifie le champ PTR ?

Exercice 36. À part pour le choix d'un serveur racine, est-ce qu'il n'existait qu'un seul chemin possible ?

Exercice 37. Que fait la commande `dig -x 195.221.122.100` ?