

TD1

DNS domain name system

Mise en pratique de la notion de serveur de noms. Installation d'un serveur DNS « à cache seul », d'un serveur DNS menteur et d'un serveur DNS maitre¹ d'une zone dans le local.

Le temps imparti pour cette manipulation (exposé oral compris) est de l'ordre de 4h.

Conseil : *Au fur et à mesure de vos travaux complétez un document reprenant toutes vos manipulations. Insérez-y les contenus de vos fichiers de configuration et expliquez vos démarches et/ou les problèmes que vous avez rencontrés ainsi que les solutions et les moyens utilisés afin de les résoudre.*

Ce document vous sera bien utile pour vos révisions.

<u>Lectures</u>	1
<u>Serveur DNS</u>	2
<u>Serveur DNS à cache seul</u>	2
<u>Bref pas à pas</u>	2
<u>Serveur DNS menteur</u>	3
<u>Serveur DNS maitre</u>	3

Lectures

Les lectures suivantes pourront vous être utiles.

- ✕ Le syllabus du cours
 - ✕ Voir Hunt, G. (Janvier 2000). TCP/IP Administration des réseaux. O'REILLY, 3^e édition. ISBN : 2-84177-221-7 Épuisé. pp 175-179
 - ✕ La documentation locale telle que les pages de manuel (*man named*, *man named.conf*, *man dig* par exemple) et le contenu du répertoire `/usr/share/doc/bind`
-

1 Ancienne orthographe « maître » <http://www.renouvo.org>

Serveur DNS

Résolveur (serveur DNS à cache seul)

Implémentez sur votre machine un serveur DNS à cache seul.

Il s'agit donc bien d'installer un programme qui se chargera de faire la résolution de noms — la traduction d'un nom internet *example.org* en une adresse IP — et vice versa.

Testez le bon fonctionnement du serveur avec commande **dig**².

Vous pouvez choisir d'utiliser **bind9** ou **unbound**.

Avant de commencer, renseignez-vous sur le gestionnaire de paquets — le programme permettant d'installer des programmes — debian. Il s'agit de **apt**.

Serveur DNS maitre

Implémentez un serveur maitre³ pour la zone `my.esigoto.info` et la zone inverse. Mettez-y quelques champs A, AAAA et CNAME ainsi qu'un champ TXT.

Qu'écrire dans un champ TXT ?

Quelles seraient de « bonnes » valeurs pour les champs MX ?

Ajoutez DNSSEC à votre zone.

Serveur DNS menteur

Un serveur DNS peut⁴ mentir ou bloquer des résolutions de noms⁵.

Mettez en place RPZ et arrangez-vous pour que votre serveur DNS bloque <http://facebook.com> et redirige <http://google.com> vers <http://ddg.gg>.

2 Il est probable qu'il faille installer **dig**, la commande se trouve dans le paquet `dnsutils`.

3 Si vous aviez choisi **unbound** à l'étape précédente, il faudra passer à **bind9**.

4 « pouvoir » prend ici le sens d'être capable de mentir pas qu'il en a l'autorisation. Posez-vous les questions des implications politiques d'un DNS menteur ou bloquant.

5 Lire à ce sujet <http://namok.be/blog/?post/2016/10/18/quand-ton-serveur-dns-te-bloque-ou-te-ment> et <http://namok.be/blog/?post/2017/03/05/mise-en-place-dns-menteur>