TD1

Routage et DNS d*omain name system*

Mise en pratique des notions de routage et de serveurs de noms. Mise en place d'un routage sur plusieurs segments, installation d'un serveur DNS « à cache seul » et d'un serveur DNS maitre[1] *d'une zone dans le local.*

Le temps imparti pour cette manipulation (exposé oral compris) est de l'ordre de 8h.

***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.

Lectures

Les lectures suivantes pourront vous être utiles.

- ✗ Formation Linux "élémentaire" — sur base de Debian — voir la formation de Delattre (depuis 2002) http://formation-debian.via.ecp.fr/
- ✗ Voir Hunt, G. (Janvier 2000). TCP/IP Administration des réseaux. O'REILLY, 3e 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/info.php?id=1356

Organisation du travail

Topologie

Nous travaillerons en fonction de la topologie du local en maximum 4 groupes, un groupe par rangée. Chaque rangée sera appelée segment.

- ✗ segment 1 - machines 5, 6 et 7
- ✗ segment 2 - machines 8,9 et 10
- ✗ segment 3 - machines 11, 12 et 13
- ✗ segment 4 - machines 14, 15 et 16

Vous choisirez une machine par segment qui servira de routeur et une autre de serveur de noms.

logging

Prenez la bonne habitude de surveiller vos services, votre machine. Pour ce faire, vérifiez les fichiers journaux (les logs) régulièrement. Le plus simple est d'ouvrir et de laisser ouverte une console dans laquelle défilent les logs. Dans cette console, il suffit d'entrer la commande :

```
tail -f /var/log/syslog
```

et les *logs* défileront sans cesse ...

Routage

Commençons par mettre en place un **routage statique** du local. Les machines 5,8,11 et 14 joueront le rôle de routeur pour leur segment respectif. Ces machines garderont leur IP 192.168.210.i pour l'interface sur le réseau 192.168.192.0/18 et prendront une IP sur l'autre segment comme présenté sur la figure.

Les différents segments se trouveront dans les réseaux[2];

segment 1	segment 2	segment 3	segment 4
172.16.0.0/18	172.16.64.0/18	172.16.128.0/18	172.16.192.0/18

Les machines sont configurées pour demander leur configuration réseau à un serveur DHCP. Il faudra désactiver cette requête en utilisant la commande `dhclient`.

Ensuite :

- les commandes `ip a` – anciennement ifconfig – et `ip r` – anciennement route – permettront de paramétrer la carte reseau et la table de routage ;

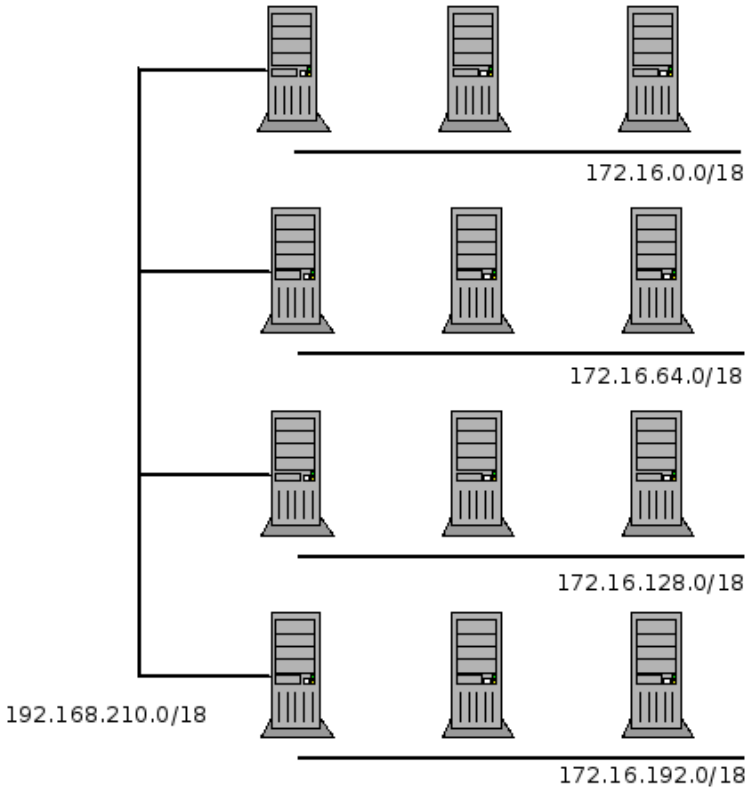
2 N'hésitez pas à vérifier que les choix de réseaux sont cohérents ... et justifiez-les dans votre rapport.

- le routeur devra laisser passer les paquet IP pour agir en tant que passerelle. Cela se configure en mettant à 1 le contenu de `/proc/sys/net/ipv4/ip_forward` ;
- pour que les réponses aux paquets sortants sur la passerelle puissent être livré à la bonne machine, ils doivent être marqués à leur sortie. C'est le firewall qui s'en charge en « faisant du NAT » via

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE.
```

> Prenez le temps de vous renseigner sur :
>
> - la commande `ip` ;
> - sur le concept de **NAT**.

Remarque. Profitez-en pour consulter vos tables arp (en passant).



Serveur DNS

Serveur DNS à cache seul

Implémenter sur chaque machine un serveur DNS à cache seul. Vous vous baserez sur :

- ✗ les *slides*, les références ;
- ✗ les *how-to* (bind9, dig…) ;
- ✗ (les pages de manuel `man named.conf` par exemple).

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

Vous testerez un maximum de « notions ». Par exemple ;

- ✗ visualisation du cache de `named ;`
- ✗ (contrôle par `rndc`)

> Avant de commencer, renseignez-vous sur le gestionnaire de paquets — le programme permettant d'installer des programmes — debian. Il s'agit de **apt**.
>
> Prenez le temps de tester `dig` en détail.

Bref pas à pas

La démarche se résume en une série de vérifications (dépendantes de la version du logiciel installé) car *debian* fait (presque) tout le boulot lors de l'installation du paquet.

1. Installation[3] du paquet *bind<i>* (ou *named*).
2. Vérification de la localisation des divers fichiers de configuration. Ils se trouvent généralement dans un répertoire du type `/etc/bind/`.
   - `named.conf`, fichier de configuration de base,
     - Vous pourrez paramétrer `bind` afin qu'il soit plus loquace, pour ce faire ajouter une section *logging* de la forme,

```
logging {
    category default { default_syslog; default_debug; };
    category security { default_syslog; default_debug;   };
    category database { default_syslog; default_debug;   };
    category resolver { default_syslog; default_debug;   };
    category queries { default_syslog; default_debug;    };
    category unmatched { null ; };
};
```

     - Attention avec ces options, vos log deviennent très verbeux… pensez à commenter ces options avant de quitter le laboratoire.

3 Avant d'installer un paquet, renseignez vous bien sur le gestionnaire de paquet *debian.*

- `db.root`, `db.local`, ...

3. Démarrage du dæmon, `service`[4] `bind start`[5] et vérification éventuelle de son existence via un `ps aux | grep named`
4. Configuration du (d'un) résolveur. Édition du fichier `/etc/resolv.conf` signalant quel serveur DNS interroger[6]
5. Test du serveur via les commandes `ping`, `dig`, ...

Serveur DNS maitre

Implémenter, pour chaque segment un serveur maitre.
Votre zone s'appelle *<segmenti>.esigoto.info*[7] et vos machines portent leur nom habituel.

Pour ce faire, vous devrez ajouter deux fichiers de zones à votre configuration. Renseignez-vous bien d'abord sur le format de ces fichiers.

Vous effectuerez vos tests localement dans un premier temps et ensuite vous interrogerez les serveurs DNS des segments voisins. Vous devez pouvoir atteindre toutes les machines sur tous les segments.

Serveur DNS menteur

Un serveur DNS peut[8] mentir ou bloquer des résolutions de noms[9].

Arrangez-vous pour que votre serveur DNS bloque http://facebook.com et redirige http://google.com vers http://ddg.gg.

4 Il existe plusieurs manières de faire : systemctl, service, invoke-rc.d ou encore /etc/init.d/ (vous préfèrerez service et systemctl).
5 Probablement *bind9*
6 Attention sur certains serveurs, ce fichier se met à jour automatiquement. Il faut donc le contrôler régulièrement !
7 `esigoto.info` est un nom de domaine à l'usage des labos d'administration
8 « 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.
9 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