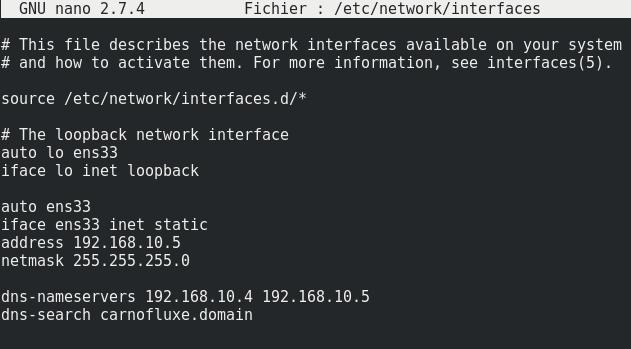
**Procédure d’installation et de configurations des serveurs DNS**

***Configuration du serveur DNS maitre :***

Pour configurer ce serveur, nous avons utilisé un paquet qui s’appelle « bind9 » et pour le télécharger, nous avons utiliser la commande :

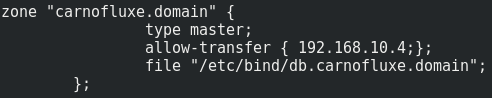


Une fois que le paquet « bind9 » est installer, nous avons donné au futur serveur DNS une adresse IP statique et pour cela nous sommes allés dans le fichier /etc/network/interfaces et taper plusieurs commandes permettant d’avoir une adresse IP statique :

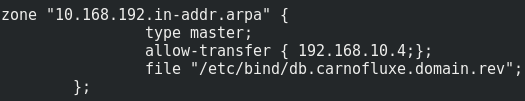


Maintenant que la machine possède une adresse IP statique (192.168.10.5) et un masque de sous réseau (255.255.255.0), la configuration du serveurs DNS peut commencer.

Pour commencer, nous sommes allés dans le fichier /etc/bind/named.conf.local pour définir les zones qui vont être utilisées. Une zone directe et une zone réverse. Pour la zone directe, nous avons entrés ces lignes dans le fichier :



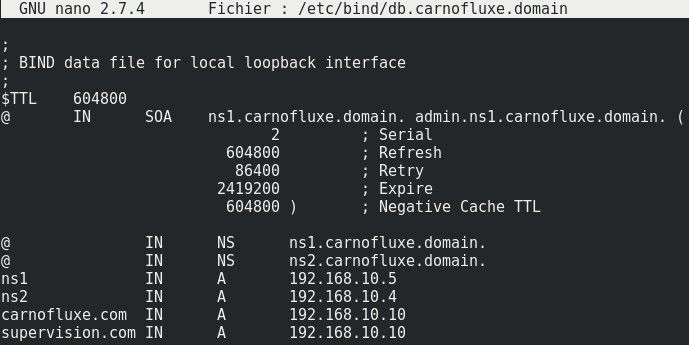
Une fois que cela est fait, la zone directe est configurée mais il reste encore la zone réverse. Cette zone est quasiment identique à la précédentes mais les noms de la zone et du fichier de configuration de la zone réverse ne sont pas les mêmes :



Le nom de chaque zones est entre guillemets (carnofluxe.domain et 10.168.192.in-addr.arpa), le type de zone et « master » car elle ce trouve sur le DNS maitre et non sur le DNS esclave, « allow-transfer » permet détermine l’adresse IP du serveur DNS esclave (192.168.10.4) et « file » donne la position exacte de chaque fichier de configuration DNS.

Une fois que ce fichier a été configuré, nous avons créer 2 nouveaux fichiers, le fichier de configuration du DNS direct (db.carnofluxe.domain) et le fichier de configuration du DNS réverse (db.carnofluxe.domain.rev).

Dans le fichier db.carnofluxe.domain ce trouve la configuration du DNS direct :



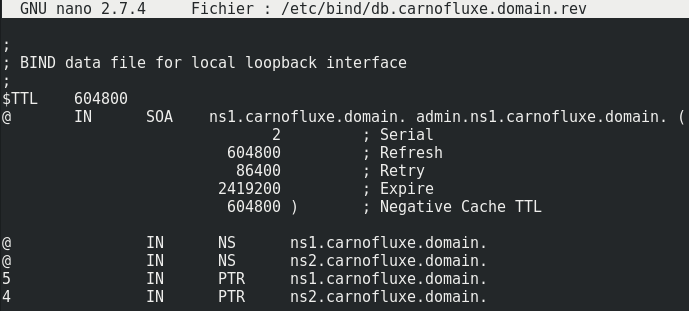
$TTL permet de déterminer la durée pendant laquelle les informations concernant le serveur DNS lorsqu’un utilisateur l’interroge seront conservées. La durée actuelle de conservation est d’une semaine et quand ce délai sera écoulé, une nouvelle demande devra être envoyée.

La ligne d’en dessous représente un enregistrement. C’est un enregistrement de type SOA (Start Of Authority) et il est suivi de plusieurs informations. D’abord, le nom du DNS maitre, l’adresse mail de l’administrateur du domaine et à la fin de la ligne, une ouverture de parenthèses pour différents paramètres et différentes valeurs.

* « Serial » permet de donner une durée entre chaque mise à jour de zone et permet d’envoyer toutes les modifications effectuées depuis la dernière mise à jour aux serveur DNS esclave. Ici, la durée est de 2 secondes.
* « Refrech » permet de donner une durée durant laquelle le serveur DNS slave stocke les enregistrements DNS sur son serveur. Ici, la durée est d’une semaine.
* « Retry » permet de donner une durée entre chaque tentative de contact du serveur DNS esclave avec le serveur DNS maitre lorsque ce dernier n’est pas joignable. Ici, la durée est de 1 jour.
* « Expire » permet de donner une limite de temps durant laquelle le serveur DNS esclave tentera de joindre le serveur DNS maitre. Ici, la durée est de 28 jours.
* « Negative » permet de donner une durée durant laquelle le serveur DNS maitre peut garder en mémoire cache les enregistrements. Ici, la durée est d’une semaine. Cette ligne est liée au TTL.

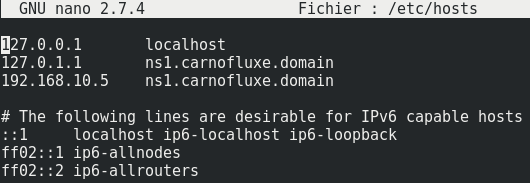
La suite de fichier sont les différents enregistrements. Pour chaque enregistrement, il y a 4 parties : l’hôte du domaine (@, ns1 et s2), la classe (IN = Internet), le type d’enregistrement (A et NS) et enfin la valeur de l’enregistrement (adresses IP et noms d’hôtes).

Nous avons ensuite configuré le DNS réverse dans le fichier db.carnofluxe.domain.rev :



Ce fichier est le même que le fichier précédant sauf en ce qui concerne la dernière partie. Les types d’enregistrements sont différents mais ils sont juste à l’envers du précédent fichier. Ns1 et ns2 ont été remplacés par le dernier chiffre de chaque adresses IP (5 et 4), les types d’enregistrements « A » ont été remplacé par PTR et toutes les valeurs d’enregistrements sont maintenant des noms d’hôtes.

Une fois que ces fichiers sont configurés, il ne reste plus qu’à configurer le fichier /etc/hosts :



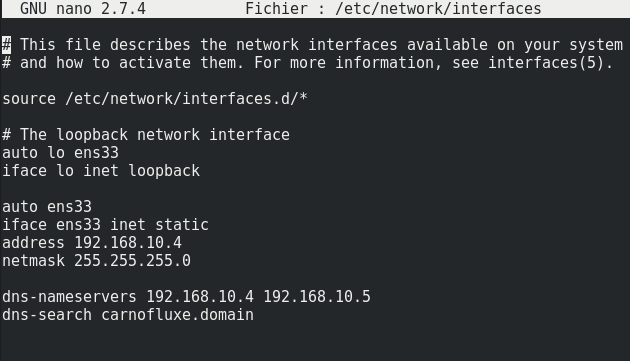
Ce fichier permet d’identifier les différents hôtes présents sur la machine virtuel.

***Configuration du serveur DNS esclave :***

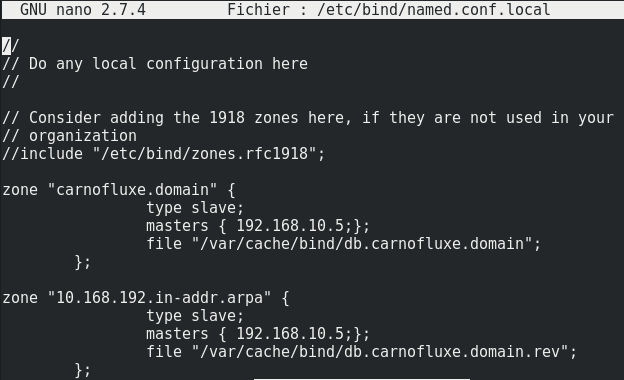
Comme pour le serveur principal, nous avons installé le paquet « bind9 » avec la commande :



Et comme pour le serveur principal, nous avons configuré une adresses IP statique dans le fichier /etc/nework/interfaces.

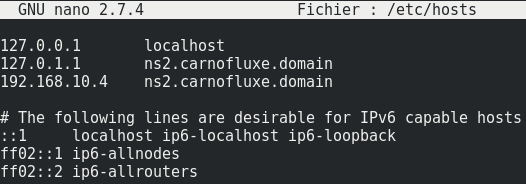


Pour finir, nous avons configuré, dans le fichier /etc/bind/named.conf.local, les différentes zones utilisées. Une zone directe et une zone réverse.



Le fichier est le même que celui qui est sur le serveur DNS maitre, les seuls choses qui change sont : le type (slave = serveur esclave) et l’adresse IP qui est celle du serveur DNS maitre (192.168.10.5).

Comme pour le DNS maitre, nous avons configuré le fichier /etc/hosts pour indiquer les différents hôtes présents sur la machine virtuelle :



Il ne reste plus qu’à rallumer le service bind9 sur le serveur DNS maitre et le serveur DNS esclave avec la commande « /etc/init.d/bind9 restart » et les 2 serveurs DNS sont prêt à être utilisés.