TD : Configuration du DNS

Principes de fonctionnement de l'architecture

- Le *Domain Name System* (ou DNS, système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.
- Le système des noms de domaines consiste en une hiérarchie dont le sommet est appelé la racine. On représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une délégation pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur. Ces sous-domaines peuvent à leur tour déléguer des sous-domaines vers d'autres serveurs. Tous les sous-domaines ne sont pas nécessairement délégués. Les délégations créent des zones, c'est-à-dire des ensembles de domaines et leurs sous-domaines non délégués qui sont configurés sur un serveur déterminé. Les zones sont souvent confondues avec les domaines.
- Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (TLD : *Top Level Domain*). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des domaines génériques (gTLD), par exemple **`.org`** ou **`.com`**. S'ils correspondent à des codes de pays (**`fr`**, **`be`**, **`ch`**, etc.), on les appelle ccTLD (*country code* TLD). On représente un nom de domaine en indiquant les domaines successifs séparés par un point, les noms de domaines supérieurs se trouvant à droite. Par exemple, le domaine **`org.`** est un TLD, sous-domaine de la racine. Le domaine **`wikipedia.org.`** est un sous-domaine de **`.org.`**. Cette délégation est accomplie en indiquant la liste des serveurs DNS associée au sous-domaine dans le domaine de niveau supérieur. Les noms de domaines sont donc résolus en parcourant la hiérarchie depuis le sommet et en suivant les délégations successives, c'est-à-dire en parcourant le nom de domaine de droite à gauche.
- L'architecture du DNS est définie dans la RFC 1034 qui est récupérable ici http://www.ietf.org/rfc/rfc1034. Son implémentation et sa spécification sont définies dans la RFC 1035 qui est récupérable ici http://www.ietf.org/rfc/rfc1035.

Mise en place

1. Ce TD utilise l'émulateur système **`QEMU`** avec le module noyau d'accélération matérielle **`KVM`** qui est installé sur les machines du CREMI. Pour configurer ces outils, il faut taper les commandes suivantes (dans cet ordre) dans un terminal :
   ```
   source /net/ens/vince/virt/nemu-init.rc
   nemu-kvm start
   ```

2. Récupérez la documentation de Vyatta située sur **`/net/stockage/dmagoni`** pour savoir comment configurer les routeurs. Les commandes de bases pour **Debian** sont aussi données dans le fichier `TD-Instructions.pdf` et celles pour **NEmu** sont dans `TD-Nemu-Guide.pdf`.
3. Ce TD utilise quatre machines virtuelles émulant des PC standards exécutant une distribution **Debian** d'un système d'exploitation GNU/Linux. Elles serviront d'hôtes ou de routeurs selon les cas. Lancez le script suivant pour démarrer ces machines :
   ```
   nemu-vnet /net/ens/vince/virt/config/netbind.py
   ```

4. Lorsqu'une machine a fini de démarrer, revenez sur la fenêtre du script et tapez sur la touche **`Entrée`**. Répétez ceci quatre fois afin de démarrer les quatre machines virtuelles.

5. Connectez-vous en tant qu'administrateur **`root`** sur chaque machine virtuelle en utilisant le mot de passe suivant : **`plop`**. Sur **Vyatta**, le login est **`vyatta`** et le mot de passe est **`vyatta`**.
6. Les commandes **Debian** et **Vyatta** données ci-dessous sont **à compléter correctement**, grâce aux documents fournis avec les images et au Web.
7. Pour chaque machine virtuelle, son interface **`eth0`** est connectée à l'Internet par SLIRP et elle est configurée par DHCP. Vous pouvez ainsi télécharger des paquets logiciels en utilisant la commande **`apt-get install`**. Pour mettre à jour la gestion des paquets, tapez d'abord **`la commande apt-get update`**.

Réseau utilisé

Un réseau intranet simple est présenté sur la figure 1a. Le réseau intranet est un réseau local de type Ethernet connecté à l'Internet via un routeur d'accès. Le réseau intranet est public, donc toutes les machines ont des adresses IP publiques.

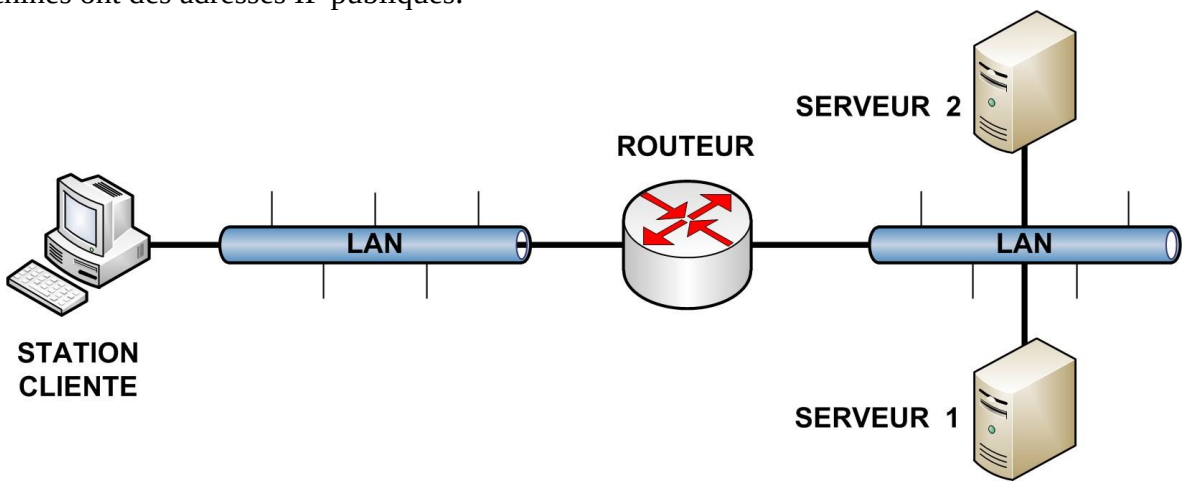

Figure 1a. Réseau étudié.

Pour le TD vous allez mettre en place la topologie présentée dans la figure 1b ci-dessous et que l'on considérera équivalente à celle de la figure 1a ci-dessus.

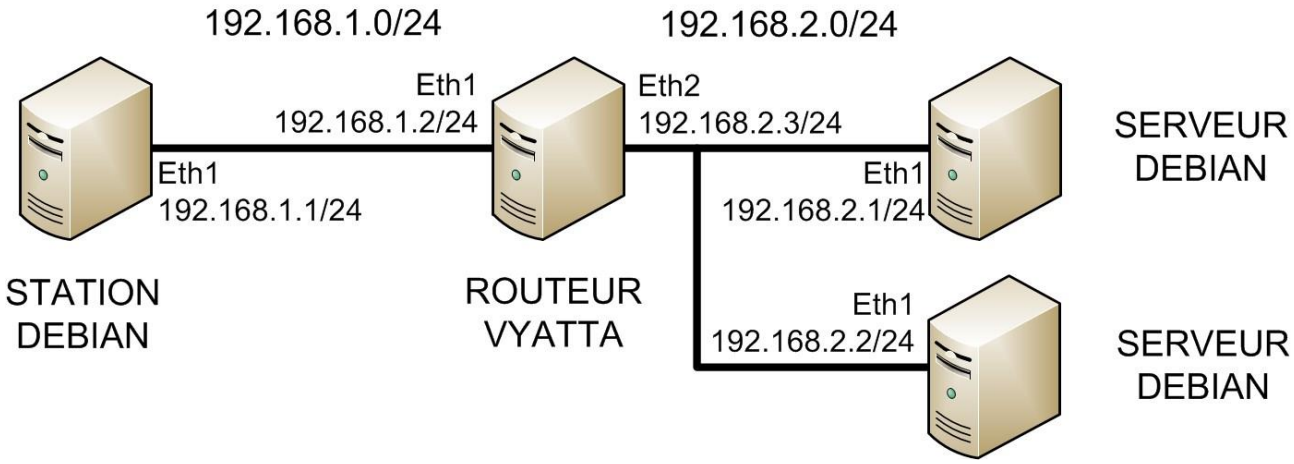

Figure 1b. Réseau 1a implémenté sur Qemu avec Debian / Vyatta.

8. Choisissez des plages d'adresses pour chaque sous-réseau. Etablir un plan d'adressage précisant les adresses de toutes les interfaces. Vous pouvez utilisez le plan d'adressage fourni sur la figure 1b si vous le souhaitez. Configurez les interfaces des machines avec **`ifconfig`**.

Configurez les interfaces des routeurs avec **set interfaces**. Vérifier les connexions directes par des **ping**. Dans la suite de ce TD, ces adresses IP sont notées **IPCL** pour le client et **IPS1** et **IPS2** pour les serveurs.

9. Remplissez les tables de routage des machines de manière statique avec **route**. Vérifiez que toutes les machines peuvent communiquer entre elles par des **ping**.
10. L'une des machines (**serveur1**) jouera le rôle de serveur primaire pour la zone **localdomain**, l'autre (**serveur2**) sera serveur secondaire de cette zone, et la troisième (**client**) sera un simple client (poste de travail). Dans un second temps, vous configurerez serveur 2 comme serveur primaire pour la sous-zone **appareils.localdomain**.
11. Installez le paquet **bind9** sur chaque serveur et le paquet **host** sur toutes les machines debian.

Résolution locale

12. Le *resolver* obtient ses informations de plusieurs sources (fichiers locaux, appel à des serveurs, base de données, etc.), selon le paramétrage indiqué dans **/etc/nsswitch.conf** à la ligne de clef **hosts**.
13. Le fichier local qui concerne la résolution est **/etc/hosts**. Modifiez celui du client pour qu'il connaisse serveur 1. Testez votre modification avec la commande **ping serveur1 -c1**.
14. Quel est le résultat de la commande **ping serveur2 -c1** ? Expliquez.

Configuration d’un serveur DNS primaire

15. Configurez **serveur1** en serveur DNS. En cas de problème, voir la fin du fichier **/var/log/syslog** via la commande **tail /var/log/syslog**. Sur **serveur1**, vérifiez que le serveur DNS tourne avec **host localhost.** (avec un point après **localhost**).
16. Lisez le fichier **/etc/bind/named.conf**
17. Sur **client**, constatez d'abord que la commande **host localhost.** échoue. Dans **/etc/resolv.conf**, ajoutez **nameserver IPS1**. Vous avez ainsi configuré le poste de travail pour qu'il utilise le serveur de nom ayant l’adresse **IPS1**. Réessayez la commande **host localhost. .**
18. Sur **serveur1**, installez **wireshark**, lancez le serveur graphique avec **startx**, puis observez avec **wireshark** les trames qui circulent lors d'une interrogation par le client. Combien de trames sont échangées ? Quels sont les protocoles et les ports utilisés ?
19. Sur le serveur, quel fichier de configuration du DNS (dans **/etc/bind/**) décrit **localhost.** ?
20. Sur **serveur1**, on va maintenant ajouter une zone **localdomain**. Copiez le fichier **db.empty** dans **db.localdomain**, modifiez le fichier **db.localdomain** comme suit pour déclarer **dns1** comme serveur de nom primaire (**dns1.localdomain.**) avec l'adresse email de l'administrateur **root.dns1.localdomain**.

```
@ IN SOA dns1.localdomain. root.dns1.locadomain. (
...
...)
```

21. Ajoutez les déclarations de **dns1** (**IPS1**), **dns2** (**IPS2**) et **poste** (**IPCL**).
22. Déclarez **dns2** comme serveur de noms de la zone. Dans **named.conf**, inspirez-vous de **localhost** pour déclarer **localdomain**.
23. Relancez le serveur de noms (commande **/etc/init.d/bind9 restart**), et vérifiez que les noms définis (**dns1.localdomain**, **poste.localdomain**, etc.) sont bien résolus.

24. Définissez un synonyme **www.localdomain.** pour **dns1.localdomain.**. N'oubliez pas d'incrémenter le numéro de série à chaque modification. Relancez et vérifiez.
25. Mettez en place la résolution inverse pour le sous-réseau IP du client ayant l'adresse x.y.z/24 (nom **z.y.x.in-addr.arpa**). Testez via la commande **host -type=ptr IPS1**

Configuration d'un serveur DNS secondaire

26. La machine **serveur2** (alias **dns2.localdomain**) va jouer le rôle de serveur secondaire pour la zone **localdomain** et la zone inverse **z.y.x.in-addr.arpa**.
27. Vérifiez que **bind9** est installé sur **serveur2**. Sur le serveur primaire, déclarez le serveur **dns2.localdomain** dans la liste des serveurs susceptibles de renseigner sur **localdomain** (ajoutez une ligne **IN NS** dans **db.localdomain**). Sur le serveur secondaire, déclarez les zones dont il est esclave, en précisant l'emplacement du fichier de stockage. Format des déclarations :

```
zone "le-nom-de-la-zone" {
      type slave;
      file "le-fichier-de-stockage";
      masters { ip-serveur-maitre ; };
}
```

28. Le fichier de stockage est créé et modifié par l'utilisateur **bind** du groupe **bind** qui n'a pas le droit d'écriture sur **/etc/bind/**. Utilisez le répertoire **/var/run/bind/run**. Relancez les deux serveurs.
29. Vérifiez que le poste de travail peut consulter les deux serveurs via la commande suivante : **host [requête] [adresse-IP-serveur-DNS]**
30. Configurez le poste de travail pour qu'il utilise les deux serveurs de nom.
31. Sur **serveur1** arrêtez le service DNS (**/etc/init.d/bind9 stop**) et vérifiez que le poste de travail peut encore résoudre les adresses. Notez le délai.

Délégation d'un sous-domaine

32. Sur le serveur primaire de la zone **localdomain**, pour déclarez un sous-domaine **appareils.localdomain** dont le serveur primaire est **dns2**, il suffit d'ajouter dans **db.localdomain** la ligne **appareils IN NS dns2**
33. Définissez cette zone sur **dns2**, avec quelques entrées pour **tele**, **magnetoscope**, **console**, etc.
34. Testez avec **host console.appareils.localdomain IPS1**
35. Et pour finir, faites tourner un serveur secondaire de cette zone sur **dns1**.

Travail à rendre

A la fin des séances de ce TD, vous rendrez un rapport de TD, au format PDF, que vous enverrez par e-mail à votre chargé de TD. Ce rapport contiendra les réponses aux questions posées dans ce sujet en y incluant tous les justificatifs nécessaires :

- Extraits pertinents des fichiers de configuration des machines **Debian** et du routeur **Vyatta**.
- Extraits pertinents des listings des commandes **Debian** et **Vyatta** utilisées pour résoudre les questions.
- Extraits pertinents des captures de trames prises par **wireshark**.