TP1 : Outils de l'administrateur réseau et installation du service DNS

Partie I : Configuration réseau d'une machine sous Linux-debian

1. Les commandes **ip link** et **ip address** permettent d'afficher et de modifier la configuration des interfaces réseaux. Identifier et indiquer les différents paramètres utiles à la configuration de votre interface réseau principale. La commande **ip link** permet également d'activer ou de désactiver une interface (ip link set up/down dev <if>). La commande **ifconfig** permet également d'obtenir ces informations, mais il est déconseillé de l'utiliser depuis qu'elle est dépréciée.

2. Les commandes **ip route** et **ip -6 route** permettent d'afficher et de manipuler les tables de routage de votre système. Quelles sont les passerelles IPv6 et IPv4 par défaut ? Expliquer l'utilité de chaque route, en expliquant notamment comment ces tables sont utilisées pour faire transiter les paquets depuis et vers Internet.

3. Ubuntu (version desktop) utilise un service spécifique pour gérer les interfaces réseaux : **network-manager**. Pour pouvoir utiliser les fichiers de configuration classiques, nous devons paramétrer ce service en éditant le fichier /etc/NetworkManager/NetworkManager.conf et en passant l'option *managed* à true, puis en redémarrant le service : sudo service network-manager restart.

4. La commande **service** permet de démarrer ou d'arrêter des services du système d'exploitation. Elle fait appel aux scripts se trouvant dans /etc/init/ ou /etc/init.d/. Tout ou partie des services sont chargés en fonction du niveau d'exécution du système (runlevels) défini dans /etc/rcX.d. **initctl list** permet de lister l'état des services. Retrouver les propriétés du service **networking** (niveaux d'exécution, priorités) et indiquer où se trouvent les commandes liées à l'exécution des scripts (start, stop, etc.). Il faut noter que les commandes service (*SysVinit*) et initctl (*upstart*) sont dépréciées dans les versions récentes de la grande majorité des distributions GNU/Linux. Elles sont remplacées par la commande systemctl (*systemd*).

5. La configuration des interfaces réseaux est enregistrée dans le fichier **/etc/network/interfaces** (ou /etc/sysconfig/network dans certains systèmes). Il permet de pérenniser les différents paramètres identifiés précédemment. En vous inspirant de l'exemple ci-dessous, configurer manuellement votre interface réseau.

```
auto eth0
iface eth0 inet6 static
    address fdfb:7689:807a::
    netmask 48
    gateway fe80:[...]
iface eth0 inet static
       address 192.0.2.7
       netmask 255.255.255.0
       gateway 192.0.2.254
```

Pour générer une adresse IPv6 de type ULA (équivalent aux adresses privées), le site *http://unique-local-ipv6.com* peut être utile. La gateway débutant par fe80 doit correspondre à celle de du routeur de la salle réseau.

Redémarrer votre interface : sudo service network-interface restart INTERFACE=ethx (ou faire un down - avant de faire les modifications - puis un up de l'interface).

Si nécessaire, configurer la table de routage de votre machine (ip route add default gw <ip> dev <if>).

6. De nombreux autres utilitaires ou commandes systèmes constituent la boite à outil de l'administrateur. Pour chacune des commandes listées ci-après, lire la page de son manuel, donner son utilité, expliquer son fonctionnement et donner un exemple d'utilisation : **ping/ping6**, **traceroute**, **netstat**, **nmap**, **host**

7. **ssh** est un utilitaire fondamental qui permet de se connecter de manière sécurisé (à travers une connexion TLS) à un hôte distant (voir également son corollaire scp). Installer et paramétrer un serveur ssh. Tester son bon fonctionnement en se connectant à l'ordinateur d'un voisin et en exécutant la commande **eject**.

Partie II : Configuration du service DNS

II.1. DNS côté client

Rappel: reprendre les slides de 76 à 89 du cours de RS présentant le service DNS.

1. Observer avec Wireshark les requêtes DNS générées lors de la consultation de sites web. Expliquer l'utilité de ce service.

2. Configurer votre service de résolution afin qu'il utilise des serveurs alternatifs (par exemple, ceux de Lorraine Data Network : 2001:913::8 et 80.67.188.188). Rajouter deux lignes *nameserver* dans le fichier **resolv.conf**. Pour empêcher le network-manager d'interférer, commenter la ligne #dns= dsnmasq dans NetworkManager.conf. Vérifier la bonne prise en compte du nouveau serveur DNS avec Wireshark.

3. Montrer comment la résolution locale avec le fichier **/etc/hosts** peut prendre le pas sur le service DNS. Quel en est l'impact est terme de sécurité? Pour information, l'ordre de consultation des bases de données est défini dans le fichier /etc/nsswitch.conf.

4. **dig** permet d'envoyer des requêtes DNS et de consulter les réponses. **nslookup** et **host** proposent un service similaire mais moins complet. A l'aide de l'outil dig (il n'est pas installé par défaut, et il possible de déterminer le paquet à installer pour pouvoir l'utiliser grâce à la commande **apt-file search -x 'bin/dig$'**), effectuer différents types de requêtes DNS (directe, inverse, mail exchange, name server, etc.). Pour chaque requête, expliquer les éléments de réponses donnés.

5. Interroger l'annuaire DNS inversé avec la commande **whois** pour obtenir des informations relatives à quelques domaines de votre choix.

II.2. DNS côté serveur

1. Installer le programme Berkley Internet Naming Daemon (*sudo apt-get install **bind9***) qui permet d'exécuter un serveur DNS.

2. Les fichiers de configuration de **bind** sont stockés dans */etc/bind/* . Configurer votre serveur comme simple relais vers le serveur DNS de TELECOM Nancy avec mise en cache des réponses : décommenter la section *forwarders* du fichier *named.conf.options*.

3. Configurer ensuite votre machine afin d'utiliser le nouveau serveur de résolution. Capturer une requête DNS avec Wireshark et vérifier qu'elle passe bien par votre serveur.

4. A l'aide d'une nouvelle capture de paquets, illustrer le bon fonctionnement du serveur relais. Quel est l'utilité de ce type de serveur ?

5. Configurer le serveur bind afin qu'il permette la résolution directe des machines de votre zone *binomeX.bootcamp.telecomnancy.eu*. Pour cela, ajouter la zone suivante au fichier *named.conf.local*

```
zone "binomeX.bootcamp.telecomnancy.eu" {
    type master;
    file "/etc/bind/db.binomeX.bootcamp.telecomnancy.eu ";
};
```

   Créer ensuite le fichier de renseignement du domaine en vous inspirant de *db.local* .
   Tester le bon fonctionnement.

6. Faire de même avec la résolution inverse en créant la zone suivante et en vous inspirant du fichier *db.127* pour créer le fichier correspondant. Vérifier avec **dig -x** la résolution inverse.

```
zone "X.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "/etc/bind/db.192";
};
```

7. Configurer la seconde machine du binôme en tant que serveur secondaire de votre zone et configurer le transfert de zone entre le maître et l'esclave.
   - Au niveau du maître, il faut rajouter la clause « allow-transfer { @IP_esclave; }; » pour chaque zone (normale et inverse).
   - Au niveau esclave, il faut remplacer le « type »par *slave* et ajouter la ligne : « master {@IP_DNS_principal ;} ; »

Montrer à l'aide d'une capture comment se fait le transfert.

8. Travailler en groupe de 4 ou plus. Configurer vos serveurs pour permettre la résolution des différents sous-domaines de bootcamp.telecomnancy.eu. Créer pour cela des nouvelles zones « binomeX.bootcamp.telecomnancy.eu » avec le type *forward* et spécificer les serveurs référents dans « forwarders {@IP_DNS_autre_zone;} ; »