TP1 - Configuration à l'"ancienne" du réseau et commandes utiles

L'objectif de ce TP est d'une part de vous présenter la configuration réseau d'une machine dans l'environnement Linux, d'autre part de vous montrer quelques commandes utiles. Bien entendu, modifier la configuration réseau d'une machine suppose d'être connecté en super-utilisateur (`root`). Seules les grandes lignes des commandes seront décrites, pour avoir la syntaxe complète d'une commande on vous invite à utiliser le manuel : `man [commande]` (`[ ]` indique que c'est optionnel), exemple : `man ls`.

Beaucoup des commandes présentées se trouvent dans un chemin non défini par défaut pour un utilisateur quelconque (`/sbin`, `/usr/sbin`).

IMPORTANT 1 : changer le mot de passe de root ! !

IMPORTANT 2 : sauvegarder le pdf du sujet dans le compte `tpreseau` et vérifier que vous arrivez à l'afficher, éventuellement en installant le lecteur `evince`. C'est indispensable car vous allez perdre ponctuellement l'accès à `cours-info`.

1 Généralités

La plupart des distributions Linux, notamment Debian / GNU Linux, utilisaient jusqu'à très récemment des scripts de démarrage SysV ("système cinq"). En effet, pour tout démon (ou *daemon*), service (un serveur SSH par exemple), ou toute configuration à faire au démarrage (la configuration d'une interface réseau par exemple), était fourni un script localisé dans `/etc/init.d`. Ces scripts étant lancés avec un paramètre qui peut être `start`, `stop` ou `restart` suivant que l'on veut démarrer, arrêter ou reconfigurer un démon, service, etc.

Le terme démon décrit de manière générale un processus non invoqué manuellement, qui s'exécute en tâche de fond et qui ne demande aucune intervention de l'utilisateur. En effet, un démon n'est rien d'autre qu'un programme qui s'exécute en arrière-plan de votre système (et ce, quel que soit le système d'exploitation).

La majorité des distributions a adopté `systemd` comme remplaçant de SysV. `systemd` permet de gérer les démons, bibliothèques et autres utilitaires permettant d'avoir un système opérationnel, tout en restant compatible avec SysV. Le but est d'offrir une meilleure gestion des dépendances entre services, de permettre un chargement en parallèle de services au démarrage et de réduire les appels aux shell scripts. `systemd` est apparu dans la version stable 8.0 - `jessie` de Debian. Lors des TPs, nous verrons tout d'abord l'ancienne méthode de configuration (celle mise en place lors de l'installation) qui s'appuie sur `ifupdown` et plus tard la nouvelle (ou "moderne"), puisque nous utiliserons la version stable 12 - `bookworm`. Cette dernière utilise soit des outils graphiques tels que `network-manager` ou `wicd` pour gérer la configuration, soit des outils de `systemd`.

Mettre une machine en réseau requiert plusieurs étapes :

1. donner un nom à la machine et indiquer un nom de domaine dans le cas d'une machine avec une adresse IP publique ;
2. *installer (éventuellement) au niveau logiciel la carte réseau (pilote et / ou firmware) ;*

3. spécifier une adresse IP / logique pour l'interface réseau associée à la carte réseau et un masque (ou préfixe) de réseau. Vous découvrirez le rôle du masque / préfixe plus tard.
   - Sous Linux, les interfaces Ethernet avaient traditionnellement pour noms `eth0`, `eth1`, etc. L'affectation des interfaces dépendant de l'ordre dans lequel les composants ont été installés. Cependant, `systemd - udev` utilise des noms d'interfaces réseau "prévisibles"(*Predictable Network Interface Names*) semblables à celui qui désigne la carte réseau de votre machine, soit `eno1`. Il est possible de modifier cette façon de faire, pour ceux que cela intéresse je les invite à consulter le manuel via `man systemd.link` ou encore `man 7 systemd.net-naming-scheme`.
   - `lo` (pour *loopback*) est l'interface de rebouclage locale. Celle-ci est utilisée pour faire des essais, ainsi que par quelques outils réseaux. Elle permet d'établir une communication TCP/IP de la machine avec elle-même.
   - Il est également possible de bénéficier d'une configuration dynamique par l'intermédiaire d'un serveur DHCP (***D**ynamic **H**ost **C**onfiguration **P**rotocol*).
4. configurer le routage, en spécifiant l'adresse IP de la passerelle (*gateway*) par défaut, généralement pour atteindre Internet. La passerelle (ou routeur) par défaut est un équipement qui appartient à plusieurs réseaux et qui permet donc à des machines d'un réseau de communiquer avec celles d'un autre réseau qui est atteignable ;
5. préciser l'adresse de serveurs de noms ou DNS (***D**omain **N**ame **S**erver*) pour obtenir l'adresse IP d'une machine connaissant son nom symbolique. Par exemple, pour `cours-info.iut-bm.univ-fcomte.fr` on obtiendra l'adresse IP `194.57.86.196`.
   - Dans le cas d'un réseau local, en l'absence de DNS, le fichier `/etc/hosts` doit fournir l'association entre adresse IP et nom symbolique pour chaque machine du réseau que l'on veut pouvoir atteindre.

2 Remplacement des commandes `net-tools` par `iproute2`

En association avec `ifupdown` on trouvait différentes commandes fournies par le package `net-tools`, commandes qui sont maintenant dépréciées (ou "obsolètes"). En effet, le package `iproute2` remplace le package (ou paquet) `net-tools` qui n'est, a priori, plus maintenu. Aussi, les commandes que contient `net-tools`, comme `ifconfig`, `netstat`, etc., qui même si elles sont toujours fonctionnelles, devraient être de moins en moins utilisées. À la place, les équivalents d'`iproute2`, décrits dans le tableau qui suit, sont donc à privilégier. Il est cependant toujours possible d'installer explicitement le package `net-tools` si on veut continuer à utiliser les commandes qu'il contient.

net-tools	**iproute2**	**net-tools**	**iproute2**
`arp -a`	`ip neigh`	`netstat`	`ss`
`arp -n`	`ip neigh`	`netstat -i`	`ip -s link`
`ifconfig`	`ip link`	`netstat -g`	`ip maddress`
`ifconfig -a`	`ip address show`	`netstat -l`	`ss -l`
`ifconfig -help`	`ip help`	`netstat -r`	`ip route`
`ifconfig -s`	`ip -s link`	`route add`	`ip route add`
`ifconfig eth0 up`	`ip link set eth0 up`	`route del`	`ip route del`
`ipmaddr`	`ip maddress`	`route -n`	`ip route show`
`iptunnel`	`ip tunnel`		

3 Interfaces réseau

L'objet de cette section est de voir comment afficher la liste des interfaces réseau d'une machine et comment en activer / désactiver une. On abordera l'utilisation de `ifconfig` pour faire cela dans la section suivante.

3.1 Liste des interfaces réseaux d'une machine

Les manipulations à effectuer sont :

1. lancer un premier terminal, puis un second terminal dans lequel vous passez `root` avec `su -`. Ce second terminal sera à utiliser pour faire les manipulations en tant que `root` ;
2. ne pas oublier de modifier le mot de passe de `root` ;
3. la première possibilité est d'utiliser la commande `ls -l /sys/class/net` ;
4. la deuxième est `ip link` ou en version courte `ip l` ;
5. plus spécifiquement pour les interfaces sans fil (*wireless*), il y a la commande `iw dev`. Il existe d'autres commandes spécifiques pour ce type d'interface : `iwconfig`, `iwlist`, etc.

3.2 Activation / désactivation d'une interface

Les manipulations à effectuer sont :

1. afficher le statut de l'interface réseau de votre machine avec `ip link show dev eno1` ;
2. désactivation de l'interface avec `ip link set eno1 down`, vérifier le nouveau statut ;
3. réactiver l'interface et vérifier que le statut est bien revenu dans l'état adéquat.

4 Étude de la configuration actuelle (à l'ancienne) d'une machine de la salle de TP

4.1 Nom

La commande `hostname` donne le nom de la machine, `uname` permet également de l'obtenir. À noter qu'il ne s'agit pas du nom symbolique complet qu'une machine aurait sur Internet.

Les manipulations à effectuer sont :

1. utiliser les commandes `hostname`, `hostnamectl` et `uname` (quelle est l'option à utiliser ?) pour afficher le nom de la machine ;
2. dans quel fichier du répertoire `/etc` est stocké le nom de la machine ?
3. comment faire pour changer le nom d'une machine ? Regarder comment faire avec `hostname`, puis avec `hostnamectl`, pour que le nom devienne `tpreseauX` où `X` est le numéro de votre machine (écrit au crayon près du logo en bas à droite de l'écran). Quelle est la différence entre les deux ?

4.2 Adresse IP et masque / préfixe de réseau

À l'issue de l'installation, `systemd` est bien activé et le `network-manager` bien présent dans la barre, mais la définition de l'adresse IP et du masque / préfixe de réseau se fait encore à l'ancienne via `ifupdown` et le fichier `/etc/network/interfaces` associé. Le masque de réseau

permet notamment de savoir si une machine destinataire d'une transmission est dans le même réseau que la machine source (l'émetteur du datagramme, ou paquet, qui est transmis).

Pour commencer, nous allons simplement regarder la configuration actuelle avec les anciennes commandes `ifconfig` et `route`. Puis nous l'étudierons avec la nouvelle commande `ip` qui permet d'obtenir des informations équivalentes avec différentes options.

Les manipulations à effectuer sont :

1. cliquer sur l'icône du `network-manager` (en haut à droite juste à la gauche de la date du jour) dans la barre et regarder ce qui est indiqué ;
2. si le `network-manager`, n'est pas installé, l'installer via `apt install network-manager` (voir NetworkManager). Si on veut pouvoir faire la configuration du `network-manager` via l'interface graphique (i.e. l'icône), il faudra également installer un autre package : `network-manager-gnome`. Pour aller plus vite, il suffit d'installer directement le package `network-manager-gnome` car il impliquera l'installation des deux packages. Après l'installation, le plus simple est de rebooter la machine ;
3. le `network-manager` donne également accès à un outil de configuration en ligne de commandes `nmcli` et un autre via une interface texte, à savoir `nmtui`. Lancer ces deux commandes pour voir ce qu'elles affichent. Nous ne les utiliserons pas lors de ce TP.
4. installer le package `net-tools` (il est peut être déjà installé).

La commande `ifconfig` et son équivalent `ip` permettent de consulter les adresses MAC / physique, ou Ethernet dans notre cas, puisque le réseau local est de ce type, et IP, le masque (ou préfixe) de réseau, l'adresse de diffusion / *broadcast* du réseau. Ainsi qu'on le verra ci-après, ces informations peuvent également être définies par la commande `ifconfig` et donc `ip`. Toutefois, ces paramètres (ou la façon de les obtenir) sont habituellement précisés, pour chaque interface de réseau, dans le fichier `/etc/network/interfaces` dans le cas d'une configuration à l'ancienne.

Les manipulations à effectuer sont :

1. utiliser la commande `ifconfig` pour répondre aux questions suivantes
   — Quelle est l'adresse IPv4 de la machine
   — Quelle est l'adresse IPv6 de la machine ?
   — Quelle est la valeur de l'adresse MAC / physique / Ethernet ?
   — Quel est le rôle de l'adresse `broadcast` (regarder ce qui se passe en utilisant la commande `ping` avec cette adresse) ?

   Remarque : si `ping` ne donne rien, regarder le positionnement des variables systèmes dont le nom commence par `icmp_echo` dans `/proc/sys/net/ipv4`, puis faire la ou les modification(s) nécessaire(s) si besoin. Voici un exemple de deux commandes équivalentes permettant de positionner la variable `ip_forward` à `1` (activation).

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   sysctl net.ipv4.ip_forward=1
   ```

   La commande `sysctl` permet de rendre le changement permanent ;
2. regarder les affichages produits par `ifconfig -a` et `ifconfig -s`, puis utiliser les commandes équivalentes avec `ip`. Il faut plus particulièrement regarder comment une même information est affiché suivant la commande utilisée ;
3. "désactiver" l'interface réseau (désignée ici par `eth0` ; donc à adapter) via

   ```
   ifdown eth0
   ```

puis après avoir vérifier la disparition de l'adresse IP avec `ifconfig -a`, la réactiver avec

```
ifup eth0
```

Regarder les information affichées lors de la configuration.
Il est possible de désactiver l'interface avec `ifconfig`, via :

```
ifconfig eth0 default down
```

ATTENTION : le remplacement de `ifconfig` par `ip link` ne permet pas de désactiver la configuration IPv4 de l'interface, car celle-ci est configurée à l'ancienne. En revanche, on peut supprimer ou ajouter une adresse IPv4 avec `ip`.

4. déduire du contenu du fichier `/etc/network/interfaces` comment se déroule la configuration de l'interface réseau ;
   Remarque : le format de ce fichier pour une configuration IPv4 est le suivant

   ```
   <mode> <interface>
   iface <interface> inet <method>
           <option> <value>
   ```

   — `<mode>` est le mode d'activation de l'interface (typiquement `auto` ou `allow-hotplug`) ;
   — `<interface>` est le nom de l'interface à configurer ;
   — `<method>` est la méthode d'attribution de la configuration pour cette interface soit `dhcp` (dynamique) ou `static` (statique).

   Nous reviendrons plus tard sur le contenu de ce fichier.
5. afficher la table de routage actuelle avec `route` ou `netstat -r` et en déduire l'adresse IP de la passerelle par défaut ;
6. modifier, grâce à `ifconfig`, le paramétrage réseau de la machine comme suit
   — adresse IP : `192.168.0.X` où `X` est le numéro de votre machine multiplié par 10 (par exemple, pour la machine `1` cela donnera `192.168.0.10`)
   — masque de réseau : `255.255.255.0`.
   Désactiver préalablement l'interface réseau. Pouvez vous encore atteindre Internet ? Pourquoi à votre avis ?
7. supprimer le paramétrage précédent en utilisant toujours la commande `ifconfig`, puis le remettre à nouveau en place avec `ip`. Pour cela, consulter le manuel et les informations données par `man ifconfig`, `ip address help` ou `man ip-address` ;
8. modifier le fichier `interfaces` avec l'éditeur `nano` pour reconfigurer l'interface réseau avec une adresse IPv4 statique et permettant d'atteindre Internet. Il s'agit de remplacer la ligne `iface ... inet dhcp` par ce qui suit en remplaçant `eth0` par le bon nom d'interface et `X` par le numéro de votre machine multiplié par 10.

   ```
   allow-hotplug eth0
   iface eth0 inet static
           address 172.20.20.X
           netmask 255.255.255.0
           network 172.20.20.0
           broadcast 172.20.20.255
           gateway 172.20.20.254
   ```

9. rebooter la machine, puis après vous être reconnecté, vérifier avec `ip` que la configuration correspond bien à ce qui a été spécifié dans le fichier `interfaces` ;

10. compter le nombre de machines répondant au `ping` sur l'adresse de *broadcast* / diffusion. **ATTENTION :** cette question et celles qui suivent n'ont de sens que si tout le monde en est à ce point de l'énoncé. De plus, suite au reboot il faudra peut-être remettre la variable `icmp_echo_ignore_broadcasts` à `0`, à moins que vous ayiez utilisé `sysctl` (cf. page 4) ;
11. ensuite, modifier le masque de réseau avec `255.255.255.224` et déterminer la valeur équivalente du préfixe en affichant la configuration de l'interface avec la commande `ip` ;
12. compter à nouveau le nombre de machines répondant au `ping` sur l'adresse de *broadcast* / diffusion. Qu'en déduisez-vous sur le rôle du masque / préfixe ?

4.3 Contrôle de la configuration et de l'activité réseau

Nous allons maintenant nous intéresser à `netstat` qui est utile pour contrôler la configuration et l'activité réseau. Par exemple, `netstat -r` affiche la table de routage et `netstat -i` des statistiques sur les interfaces configurées. **En plus de `netstat`, vous regarderez les équivalents du package `iproute2`** (cf. le tableau du bas de la page 2).

Les manipulations à effectuer sont :

1. se connecter avec `ssh` sur une machine distante et afficher la page de `cours-info` avec un navigateur, puis utiliser la commande `netstat` sans aucune option, mais en filtrant avec `more`, via `netstat | more`.
   Quelles sont les informations affichées ?
2. afficher la table de routage, que donne-t-elle comme informations ?
3. quelle est en octets la valeur du MTU (*Maximum Transmission Unit*) affichée par la commande `netstat -i` ?
4. qu'affiche la commande `netstat -l | more` ?
5. qu'affiche la commande `netstat -a | more` ?
6. refaire les manipulations précédentes en utilisant les commandes équivalentes d'`iproute2` ;
7. `netstat -atpn | more` et son "équivalent" `ss -nape` permettent d'avoir un affichage avec de nombreuses informations. Exécuter ces deux commandes et regarder / analyser les informations données.

4.4 Table ARP

Le protocole ARP (***A**ddress **R**esolution **P**rotocol*) permet à un hôte de trouver l'adresse MAC / physique de l'hôte destination connecté au même réseau physique et dont on connaît l'adresse IP. Ce protocole est notamment utile pour transmettre des données directement entre deux machines connectées au même réseau physique.

Les manipulations à effectuer sont :

1. afficher successivement la table ARP avec les commandes `arp` et `ip` (en utilisant la bonne option) ;
2. installer le package `wireshark` et répondre `Oui` pour autoriser les utilisateurs non privilégiés à l'utiliser ;
3. dans le terminal `root` exécuter la commande `usermod -aG wireshark tpreseau` ;
4. fermer la session, puis se reconnecter et lancer les deux terminaux comme au début ;

5. vérifier que `tpreseau` a bien `wireshark` dans la liste des groupes auxquels il appartient avec la commande `id` ;
6. démarrer `wireshark` pour observer comment la machine récupère l'adresse physique d'une machine. Pour ce faire, au niveau de l'item `Capture`, vous indiquerez au niveau des options le filtre de capture suivant : `arp`.

   ATTENTION : il s'agit du `capture filter` et non du `display filter` plus haut.
7. utiliser `ping` pour contacter une machine, faisant partie de votre réseau, dont l'adresse IP ne se trouvait pas dans la table ARP, ensuite réafficher la table ARP ;
8. arrêter la capture des trames dans `wireshark` et étudier les trames relatives à l'ARP.

4.5 Le *Domain Name System*

Le principe du DNS sera revu lors du Cours / TD de la ressource R2.05.

4.5.1 Introduction

- Lorsque des machines communiquent dans un réseau informatique, c'est toujours par le biais d'adresses IP (source, destination).
- Ces adresses sont difficilement mémorisables et ne permettent pas de souplesse dans la configuration. En effet, se souvenir d'une adresse comme `77.245.141.172` n'est pas aisé, alors que la mémorisation du nom symbolique `www.iut-bm.univ-fcomte.fr` est beaucoup plus aisé.
- Le rôle du protocole DNS est précisément de fournir la correspondance entre adresse IP et nom symbolique. Ainsi, le service DNS permet de faire de la résolution de noms : fournir à des clients qui en font la demande l'adresse IP d'une machine connaissant son nom symbolique, et vice-versa. Par exemple, la ou les adresses IP de `www.google.com`.
- Les noms symboliques sont structurés et hiérarchiques :
  — une partie désigne le nom de la machine (*host name* - l'équivalent d'un prénom) ;
  — l'autre partie désigne le nom de domaine (*domain name* - l'équivalent d'un nom de famille) de la machine.

  Par exemple, à l'IUT on a pour nom de domaine `iut-bm.univ-fcomte.fr`. Dans chaque domaine un (ou plusieurs) serveur de noms ou serveur DNS est chargé de répondre aux requêtes des clients.
- Les informations sur les noms de domaines sont déclarées lors de l'achat ou de l'attribution d'un nom de domaine auprès d'un / par un organisme de nommage. L'accès à ces informations est libre, cela permet notamment de savoir si un nom de domaine est libre ou par qui il est utilisé. Cela se fait via la commande `whois` en donnant éventuellement un nom de serveur. De nombreux sites web permettent d'obtenir ces informations.

Les manipulations à effectuer sont :

1. installer le package `whois` ;
2. exécuter `whois univ-fcomte.fr` et `whois yahoo.com` ;
3. exécuter `whois -h whois.nic.fr yahoo.com` et `whois -h whois.nic.fr gouv.fr` ;
4. exécuter `whois 193.52.61.3`.

4.5.2 Les différents fichiers de configuration

- **Déroulement de la résolution du nom → fichier `/etc/nsswitch.conf`**
  La résolution du nom d'un hôte est actuellement pris en charge par le mécanisme NSS (*Name Service Switch*). Aussi, le fichier `/etc/host.conf` qui, historiquement, contenait l'ordre de recherche pour la résolution : habituellement d'abord la consultation du fichier `/etc/hosts`, puis l'interrogation du DNS, est désormais remplacé par le fichier `/etc/nsswitch.conf`. Toutefois, `/etc/host.conf` est toujours présent, c'est pourquoi nous allons voir en détail le contenu des fichiers `host.conf` et `nsswitch.conf`.
  — Le fichier `/etc/host.conf`
  Comme l'ordre est maintenant précisé par `nsswitch.conf`, la seule option que contient `host.conf` est *multi* qui prend les arguments *on* ou *off*. Cela indique si pour un hôte spécifié dans `/etc/hosts` il faut renvoyer toutes les adresses IP possibles ou uniquement la première (dans le cas où il y a plusieurs adresses IP). C'est en général le cas d'un hôte faisant office de passerelle entre réseaux. Pour plus d'informations sur toutes les options qui peuvent être spécifiées sur une ligne dans ce fichier, utiliser le manuel via `man host.conf`.
  — Le fichier `/etc/nsswitch.conf`
  Il donne l'ordre de résolution du nom d'hôte avec une ligne comme
  `hosts: files dns`
  qui indique que la méthode `files` et d'abord appelée, puis la méthode `dns`. La méthode `files` signifie que la résolution de nom se fait en utilisant le fichier `/etc/hosts` qui est en quelque sorte un DNS local. La méthode `dns` utilise elle un autre fichier : `/etc/resolv.conf`. Voyons maintenant ce que contiennent ces deux fichiers.
- **Résolution locale → fichier `/etc/hosts`**
  Dans ce fichier sont précisées des correspondances entre adresse IP et nom symbolique de différentes machines. On peut ainsi s'affranchir de l'utilisation d'un serveur de noms (ou DNS) pour les machines spécifiées dans ce fichier (`man hosts`).
  Ainsi, si deux machines souhaitant communiquer possèdent dans leur fichier `/etc/hosts` respectif l'adresse IP et le nom de l'autre machine (on y trouve souvent également leur propre adresse associé à leur nom) le serveur DNS ne sera pas utilisé. Cela signifie aussi qu'il n'y aura pas de communication réseau générée. En plus des correspondances, on peut définir des alias pour les machines.
  Voici un extrait du fichier `/etc/hosts` de la machine `dubrovnik`
  `193.52.61.48 zagreb.iut-bm.univ-fcomte.fr zagreb zaza`
  On indique ainsi que la machine `zagreb.iut-bm.univ-fcomte.fr` a pour adresse IP `193.52.61.48` et pour alias (ou surnoms) `zagreb` et `zaza`.
- **Résolution avec les serveurs DNS → fichier `/etc/resolv.conf`**
  Les serveurs de noms à utiliser sont spécifiés dans le fichier `/etc/resolv.conf` (`man resolv.conf`) :
  — *domain* (peut être absent) indique le domaine local à ajouter aux noms non qualifiés (ne comportant pas de domaine). Un nom complètement qualifié, ou nom de domaine complet, est aussi appelé `FQDN` pour *Fully Qualified Domain Name* ;
  — *search* fixe la liste des domaines à ajouter aux noms d'hôtes qui ne sont pas complets (en son absence la liste est construite à partir du nom de domaine local et de celui des domaines parents) ;
  — *nameserver* indique l'adresse d'un serveur de noms, trois serveurs DNS au plus peuvent être spécifiés (ils seront utilisés dans l'ordre indiqué).

Voici à quoi devrait ressembler le fichier `/etc/resolv.conf` de votre machine :

```
domain iut-bm.univ-fcomte.fr
search iut-bm.univ-fcomte.fr
nameserver 193.52.61.11
nameserver 194.57.86.193
```

Remarque : le package `resolvconf`, un complément de `ifupdown`, a été créé afin d'éventuellement automatiser la réécriture du fichier du fichier `/etc/resolv.conf`.

Les manipulations à effectuer sont :

1. consulter les fichiers `/etc/host.conf`, etc. ;
2. installer le package `dnsutils` qui contient les commandes `nslookup` et `dig` ;
3. utiliser `wireshark` pour observer comment fonctionne le protocole DNS. Pour ce faire, au niveau de l'item `Capture`, vous indiquerez au niveau des options le filtre de capture suivant : `port 53`, puis exécuter la commande `nslookup www.yahoo.fr`.

   ATTENTION : l'option précédente s'applique uniquement au filtre de capture, une fois qu'une capture est démarrée si on veut filtrer les paquets il faut passer par le *display filter* via `udp.port == 53 || tcp.port == 53`.

   Vous étudierez les différents champs de l'en-tête UDP, quelle est l'adresse IP de l'hôte hébergeant le serveur web `www.yahoo.fr`, qui a répondu ?
4. refaire la même manipulation avec `wireshark`, mais en vous connectant avec `firefox` cette fois à un site web à la place de l'utilisation de la commande `nslookup`.

4.5.3 Commandes d'interrogation

- `nslookup` permet de résoudre, par le biais d'un serveur de noms, un nom de machine en retournant son adresse IP et inversement ;
- `dig` permet de repérer des problèmes de fonctionnement d'un serveur de noms ;
- `host` permet de vérifier rapidement le bon fonctionnement de la résolution de noms.

Les manipulations à effectuer sont :

1. exécuter `nslookup www.iut-bm.univ-fcomte.fr` et `nslookup 193.52.61.135` ;
2. exécuter `dig @a.root-servers.net www.iut-bm.univ-fcomte.fr`,
   puis `dig @f.ext.nic.fr www.iut-bm.univ-fcomte.fr`
   et `dig @ufc.univ-fcomte.fr www.iut-bm.univ-fcomte.fr`.
   Que fait cette suite d'instructions et qu'obtient-on au final ?
3. pourquoi si on remplace `www.iut-bm.univ-fcomte.fr` par `slayer.iut-bm.univ-fcomte.fr` pourrait-on faire `dig @demeter.iut-bm.univ-fcomte.fr slayer.iut-bm.univ-fcomte.fr` en plus pour obtenir l'adresse IP de `slayer` ?
4. exécuter `host www.yahoo.com`, que constatez-vous comme différence avec `nslookup` ?
5. relancer la commande `host www.yahoo.com` plusieurs fois, que constatez-vous ?
6. exécuter `host -t ns iut-bm.univ-fcomte.fr`, puis `host -t mx gmail.com`.
   Que nous apprennent ces deux commandes `host` avec l'option `-t` ?

Que permet d'obtenir comme information chacune de ces commandes ?

5 Accessibilité à une machine

5.1 Commande `ping`

`ping` permet de vérifier si une machine distante répond. Néanmoins, il faut savoir qu'une réponse positive indique seulement que l'interface réseau est initialisée correctement. Ainsi, la machine peut très bien ne pas être opérationnelle du point de vue des applications réseau.

5.2 Commande `traceroute`

Cette commande permet de connaître le chemin emprunté par les paquets IP pour aller de la machine locale à la machine distante spécifiée. Par chemin on entend la suite de routeurs qui permettent d'atteindre la destination. Une alternative possible est `mtr`.

Les manipulations à effectuer sont :

1. exécuter `traceroute www.yahoo.com` ;
2. installer le package `mtr`, puis lancer `mtr` et afficher la route vers `www.yahoo.com`. Vous constaterez que cette commande donne plus d'informations ;
3. refaire la manipulation précédente avec `www.ubc.ca`.