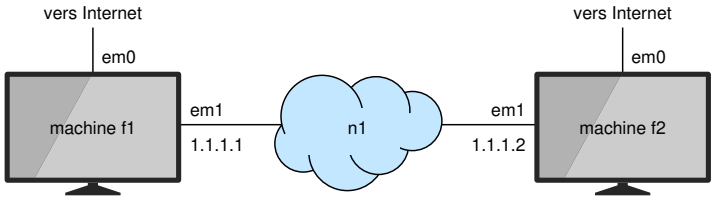
Semaine 0xA – DNS

Exercice 1

À l'aide de `dig`, donnez les adresses IPv4 et IPv6 de `ip.lafibre.info`.

Exercice 2

L'objectif de cet exercice est d'identifier les deux opérations associées à la résolution de noms, en considérant le fichier `/etc/hosts`. Pour cela, mettez en place la topologie ci-dessus :



De plus, vous devrez vous connecter avec SSH depuis `f2` sur `f1`. Pour cela, vous devrez démarrer le serveur SSH et mettre un mot de passe [1] sur cette machine. Pour ne pas vous perdre entre les différentes fenêtres, définissez le nom de chaque machine. Par exemple, sur `f1` : `sudo hostname f1`. Puis, fermez la fenêtre et ouvrez-en une nouvelle pour rafraîchir le *prompt* du Shell.

1. Sur `f2`, définissez l'adresse de `f1` dans le fichier `/etc/hosts`. Testez avec la commande `ping f1`.
   L'opération consistant à traduire un nom en une adresse IP s'appelle la « résolution de nom ».
2. Pourquoi peut-on donner plusieurs noms à une même adresse IP ? Quelle(s) utilisation(s) cela peut-il avoir ?
3. Depuis `f2`, connectez-vous avec SSH sur `f1`. Une fois connecté sur `f1`, utilisez la commande `who` pour afficher les utilisateurs et le terminal ou la machine source. Sous quelle forme `who` affiche votre provenance ?
   Comparez avec une connexion, depuis `f1`, en SSH vers `127.0.0.1`. Expliquez.
4. Faites en sorte que lorsque vous vous connectez en SSH depuis `f2` vers `f1`, la commande `who` sur `f1` réalise la *résolution de nom inverse*, c'est-à-dire affiche `f2` au lieu d'une adresse IP.
   Note : en réalité, la résolution inverse n'est pas effectuée par `who`, mais par le démon `sshd` au moment où il accepte l'ouverture de session. Si vous devez faire plusieurs essais, il faut vous déconnecter et vous reconnecter à chaque fois. Vous avez également la possibilité d'utiliser une commande qui effectue la résolution inverse au moment où vous l'appelez, comme par exemple `netstat -a -f inet` (sans le `-n` auquel vous êtes habitué).

Exercice 3

L'objectif de cet exercice est d'expérimenter l'outil simple `nslookup` de résolution de noms DNS à l'aide d'un serveur mandataire. Dans cet exercice, nous n'utiliserons que `f1`. Démarrez `wireshark` pour capturer le trafic sur l'interface `em0`.

1. Consultez le fichier `/etc/nsswitch.conf` : comment sont configurées les résolutions de noms ? Vous pouvez consulter le « man » de `nsswitch.conf`.

1. Utilisez la commande `passwd` et définissez un mot de passe simple.

2. Consultez le fichier `/etc/resolv.conf` : vous y trouverez le ou les noms de domaine servant à la recherche de noms relatifs, ainsi que l'adresse IP du serveur de noms mandataire (dans le cas de votre machine virtuelle, ce rôle est assumé par VirtualBox).
3. Utilisez la commande `nslookup turing.unistra.fr` et interprétez le résultat.
4. Identifiez avec `wireshark` les paquets échangés pour cette interrogation. Combien de paquets sont échangés ? Quel protocole sous-jacent est utilisé ? Analysez les 4 grandes sections de la question et de la réponse. Analysez les flags. Comment la question et la réponse sont-elles associées ?
5. Utilisez `nslookup` pour obtenir l'adresse de `www.renater.fr`. Que constatez-vous ?
6. La commande `nslookup` peut également être utilisée pour la résolution inverse : faites `nslookup 130.79.255.66`. Quel *Resource Record* (RR) est interrogé (nom et type) ?
7. La commande `nslookup` peut servir à interroger d'autres types de RR. Faites : `nslookup -q=ns unistra.fr` pour obtenir la liste des serveurs de noms du domaine `unistra.fr`. Combien de RR sont mentionnés dans la réponse ?

La commande `nslookup` a beaucoup d'autres possibilités, mais nous allons maintenant nous intéresser à l'outil `dig`, beaucoup plus flexible et davantage utilisé par les administrateurs DNS.

Exercice 4

Dans cet exercice, nous n'utiliserons que `dig` sur `f1`. Il n'y a à priori pas besoin d'utiliser `wireshark`.

1. En utilisation basique, `dig` est comparable à `nslookup`. Par exemple :

   ```
   dig turing.unistra.fr a
   ```

   utilise une recherche *récursive* du RR correspondant au nom et au type (ici `a`) indiqués. La commande affiche ensuite la réponse [2], avec les flags et le nombre de RR dans chaque section.

   Localisez les flags, le serveur interrogé et les différentes sections indiquées dans la réponse.
2. L'outil nous permet d'interroger d'autres serveurs de noms que notre serveur mandataire par défaut. Ici, il est demandé au serveur mandataire par défaut sur Osiris de servir de mandataire pour la requête fétiche :

   ```
   dig @130.79.200.200 turing.unistra.fr a
   ```

   Expliquez la réponse du serveur si cette requête est effectuée depuis l'intérieur d'Osiris (par exemple via une connexion SSH sur turing) ou depuis l'extérieur.
3. Essayez de poser cette même question à un serveur de noms ayant un rôle d'autorité pour un domaine, par exemple à l'un des serveurs de noms gérant le domaine `fr` :

   ```
   dig @d.nic.fr turing.unistra.fr a
   ```

   Expliquez la réponse du serveur.
4. Sachant qu'un des serveurs de noms de la racine est `a.root-servers.net` (198.41.0.4), effectuez la suite des requêtes avec `dig` pour obtenir l'adresse IP de `bambi.lptl.jussieu.fr`.
5. Comment connaître le nom associé à l'adresse 130.79.200.200 avec `dig` ?
6. En utilisant `dig`, déterminez quels sont les serveurs de noms de la zone `unistra.fr`, quelle est l'adresse à contacter en cas de problème, quel serveur est le primaire, et quelle est la version de la zone.
7. Déterminez les adresses que peut utiliser la commande `pkg` de gestion des paquets de FreeBSD : interrogez les RR de type SRV correspondant à `_http._tcp.pkg.freebsd.org`.

2. La réponse est indiquée dans un format exploitable par un serveur de noms.