Semaine 6 – TCP

Exercice 1

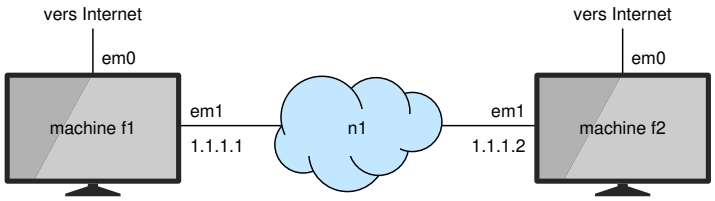
Créez une machine virtuelle `f1`. Démarrez `wireshark` sur l'interface `em0` et lancez depuis une fenêtre « terminal » la commande :

```
fetch http://130.79.201.63
```

1. Identifiez les segments TCP d'ouverture de connexion.
2. Quels sont les ports utilisés ?
3. Quels sont les numéros [1] de séquence et d'acquitement échangés ?
4. Si vous refaites la même opération `fetch`, les numéros de séquence changent-ils ?
5. Identifiez quelle partie (début, longueur) des flux de données figure dans chaque segment. Astuce : utilisez un filtre (par exemple « `ip.src == 10.0.2.15` ») pour sélectionner chacun des flux. Y a-t'il des segments sans donnée ? Pourquoi ?
   Combien de segments sont nécessaires pour que le serveur envoie toutes ses données ? Pourquoi ?
6. Identifiez les segments TCP de clôture de connexion.

Exercice 2

Reprenez la topologie simple à 2 nœuds :



Créez une deuxième machine virtuelle `f2` et connectez-la à `f1` sur le réseau interne *n1*. Sur `f1`, ouvrez deux fenêtres « terminal ». Dans chacune, ouvrez une connexion SSH sur `f2`. Une fois la clef distante approuvée, laissez la connexion ouverte, mais n'essayez pas de saisir un mot de passe : le serveur SSH refuse les connexions à des comptes ouverts. On rappelle que le numéro de port TCP du protocole SSH est 22.

Sur `f1` et `f2`, faites `netstat -an -p tcp -f inet` pour voir l'ensemble des sessions TCP :

1. Quels sont les paramètres qui permettent à `f2` de différencier la connexion du premier client SSH de la connexion du deuxième ? Même question pour `f1`.
2. Quels sont les états des connexions TCP sur `f1` ? Faites le lien avec l'automate TCP.
3. À quoi correspond la ligne « `*.22` » sur `f2` ?
4. Après 2 minutes, un serveur SSH qui ne réussit pas à authentifier un client rompt unilatéralement la connexion. Le client ne le détecte pas. Juste après cette rupture, comparez les états d'une connexion de chaque côté.
5. Ouvrez une nouvelle connexion depuis `f1` et rompez-la avec Ctrl-C. Que devient cette connexion ?

1. Pour cette question, il faut empêcher `wireshark` de vous faciliter la vie et de traduire ces numéros absolus en numéros relatifs au début de la connexion : clic droit sur un paquet TCP puis dé-sélectionner « Protocol Preferences / Analyze TCP sequence numbers ». Vous pourrez sélectionner à nouveau cette option après cette question.