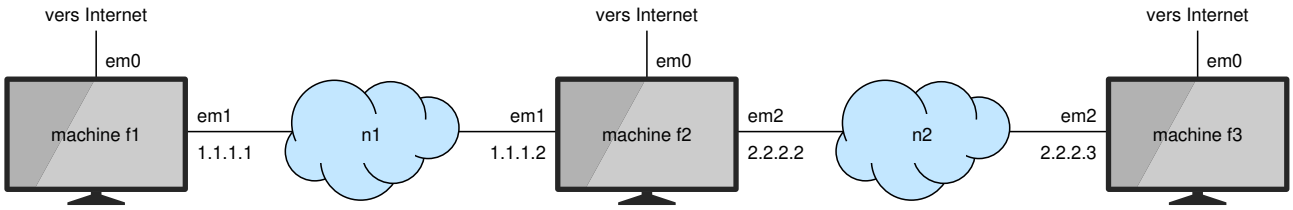
# Semaine 5 – ICMP

## Exercice 1

Reprenez la topologie à 3 nœuds :




Activez la fonctionnalité de routage sur `f2` et `f3` (rappel : `sysctl`). Démarrez `wireshark` sur `f1` et `f2` pour visualiser tout le trafic reçu et émis par ces machines.

Dans cet exercice, nous utiliserons le programme `ntpdate` qui a pour but de synchroniser l'horloge de l'ordinateur local avec un serveur de temps en utilisant des datagrammes UDP. Déjà installé, ce programme est un client UDP facile à utiliser. Vous pouvez le tester avec le serveur `pool.ntp.org` par exemple. Dans cet exercice, nous l'utiliserons avec un serveur invalide pour observer les messages ICMP.

1. Faites `sudo ntpdate 2.2.2.3` sur `f1` et arrêtez le programme après le premier échange de datagrammes. Analysez le datagramme ICMP reçu : quels sont l'adresse source, le type et le code ? Comparez le reste du datagramme ICMP avec le datagramme original.
2. Pour mettre en évidence un problème de routage :
   — ajoutez sur `f1` une route vers le réseau `4.4.4.0/24` passant par `f2`
   — ajoutez sur `f2` une route vers le réseau `4.4.4.0/24` passant par `f3`
   — désactivez la route par défaut sur `f2` et `f3` :

   ```
   sudo route delete default
   ```

   Sur `f1`, utilisez à présent `ntpdate` vers `4.4.4.4` et arrêtez le programme après le premier échange de datagrammes. Qu'est-ce qui diffère ? Expliquez.
3. Pour constituer une boucle de routage, installez sur `f3` une route vers `4.4.4.0/24` passant par `f2`. Refaites la même commande `ntpdate`. Analysez les datagrammes capturés sur `f2` et le datagramme ICMP reçu par `f1`.
4. Analysez les paquets émis et reçus par `f1` sur l'interface `em0` lorsque vous faites `traceroute -n 130.79.201.195` (adresse du serveur Web de l'université). Quelles précisions pouvez-vous apporter par rapport à l'algorithme vu en cours ?
5. Le TTL initial est modifiable en utilisant `sudo sysctl -w net.inet.ip.ttl=`$n$. Depuis `f1`, utilisez `ping` vers `f3` avec $n = 1$, puis $n = 2$.