

TP2

Tous les protocoles au dessus d'IP sont numérotés, comme TCP ou UDP. Une table est lisible dans `/etc/protocols`, trouvez-y les numéros de TCP et UDP. Les services TCP (`http`, `ftp`, `ssh`, ...) sont également numérotés (et sont appelés **numéros de port**), la table est dans `/etc/services`, trouvez-y `http`, `ftp`, `ssh`, ... Les numéros entre 0 et 1023 ne sont utilisables que par l'utilisateur `root`.

1 Netcat

- Lancez `nc -l -p 12345` et laissez-le tourner . Observez (en passant par un autre terminal) dans `netstat -Ainet -Ainet6 -a` l'apparition du service parmi les autres.
- Ajoutez à `netstat` l'option `-p` pour constater que c'est bien le programme `nc` qui est à l'écoute.
- Dites à votre voisin de lancer `nc votremachine 12345` . Observez dans `netstat -Ainet -Ainet6` la connexion établie.
- Tapez des lignes d'un côté ou de l'autre, observez que c'est effectivement transmis de l'autre côté.
- Comment transmettre un fichier d'une machine à l'autre à l'aide de `nc` et de redirection `bash` ? (utilisez l'option `--send-only` côté émetteur)

2 Services au CREMI : LDAP & NFS

Quelle que soit la machine que vous utilisez au CREMI, elle vous connaît et retrouve vos fichiers. Comment cela se passe-t-il ?

- Pour l'identification et l'authentification, c'est le protocole LDAP qui est utilisé, la configuration est lisible dans le fichier `/etc/ldap.conf` (pas la peine de tout lire, ce qui nous intéresse est au tout début), pourquoi y a-t-il plusieurs serveurs (`host`) ? Trouvez le numéro de port de ce service, vérifiez dans `/etc/services`.
- Vos fichiers sont stockés sur un serveur NFS, utilisez la commande `df ~` pour repérer le nom du serveur, et chemin sur le serveur.

3 Connexion à une machine distante avec SSH

Utilisez la commande `ssh -X` pour vous connecter sur la machine du voisin. Lancez `xeyes`, sur quelle machine s'exécute-t-il ?

Comment l'affichage se retrouve-t-il sur votre machine ?

4 Routage

4.1 Préliminaires

Pour dialoguer avec la Terre entière, il est nécessaire de passer par des passerelles. Lancez la commande `/sbin/route -n`. Il y a deux routes importantes.

- La route des machines de la salle (en `10.0.x.y`), qui sont accessibles directement en Ethernet sans passer par un routeur, remarquez le **Genmask**, il indique la séparation entre la partie réseau (bits à 1) et la partie machine des adresses IP (bits à 0). Comparez avec les adresses de vos voisins : êtes-vous bien dans le même réseau ?
- La route par défaut (`0.0.0.0`), qui utilise une passerelle (quelle est son adresse IP ?)

On peut aussi utiliser la version plus moderne `ip route ls`. À quoi correspond le suffixe `/24` ?

Pour observer en IPv6, on utilise `ip -6 route ls`. On a les mêmes deux routes importantes :

- La route des machines de la salle (en `2001:660:6101:800:x::y`), qui sont accessibles directement en Ethernet. Observez le suffixe `/80`, et comptez le nombre de chiffres hexadécimaux auxquels cela correspond dans l'adresse IP pour déterminer la partie réseau et la partie machine. (attention, les 0 non significatifs ne sont pas écrits en IPv6, chaque paquet séparé par `:` compte pour 16 bits).
- La route des adresses locales `fe80::/64` : on a sur `eth0` non seulement une adresse publique (`2001:...`), mais aussi une adresse locale en `fe80::/64`. L'une ou l'autre sera utilisée selon que l'on veut émettre en local seulement, ou bien sur le reste d'Internet.
- La route par défaut (`default`) utilise une passerelle de type `fe80::...` : c'est l'adresse IPv6 locale du routeur pour cette salle-ci.

Memento Routage

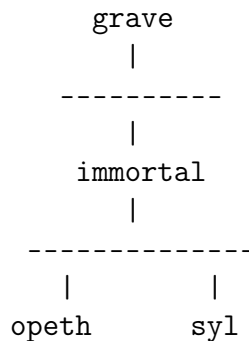
En guise de documentation rapide, voici un résumé des commandes que l'on va utiliser dans les sections suivantes. Il n'y a donc pas d'action à faire dans cette section, c'est juste de la documentation. Il faut bien sûr remplacer `<@gateway>` par une adresse IP, etc.

- Activer le relai des paquets sur une machine (`ip forward`) :
`echo 1 > /proc/sys/net/ipv4/ip_forward`
- Configurer de manière permanente le relai des paquets : voir le fichier `/etc/sysctl.conf`
- Afficher la table de routage : `route -n`
- Définir une route par défaut : `route add default gw <@gateway>`

- Ajouter une route vers un réseau spécifique :
`route add -net <@network/bits> gw <@gateway>`
- Pour supprimer une règle, il faut taper la commande `route del <...>` avec exactement les mêmes arguments que pour la commande `add`.
- Vérifier la route envoyer un paquet à une adresse spécifique : `traceroute <@host>`
- On peut aussi utiliser la commande `ip` pour ajouter des route :
`ip route add <@network/bits> via <@gateway>` (de même pour une seule adresse).

4.2 Routage Basique

Dans un LAN, toutes les machines peuvent communiquer directement, car elles sont physiquement connectées par leurs interfaces réseaux. Dans un réseau plus complexe, comme celui que nous allons étudier maintenant, il est nécessaire de configurer les tables de routage des machines, pour qu'elles collaborent à l'acheminement des messages d'un bout à l'autre du réseau.



Pour lancer la topologie ci-dessus, veuillez taper la commande suivante sur votre propre machine :

```
/net/ens/qemunet/qemunet.sh -x -s /net/ens/qemunet/demo/gw1.tgz
```

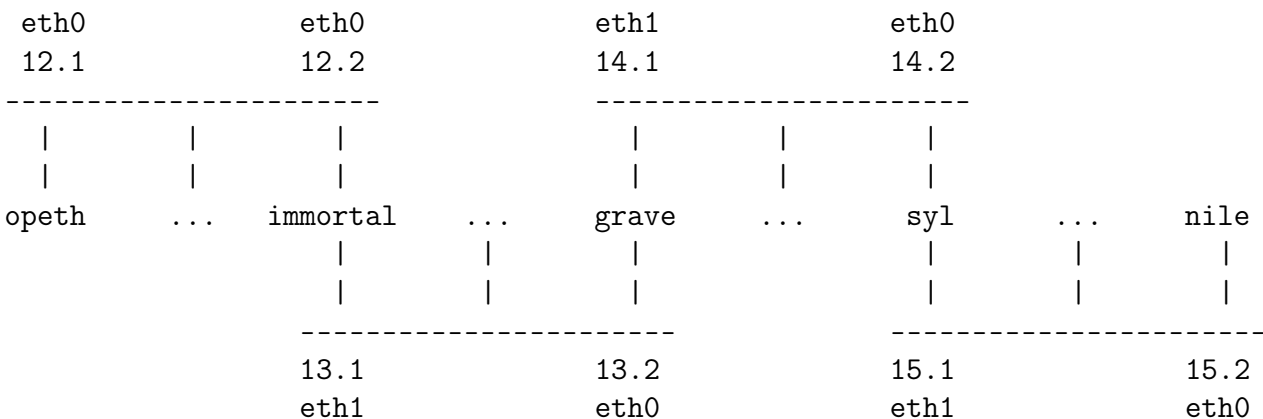
- Les adresses IPs sont déjà configurées. Veuillez reporter chaque adresse IP sur le schéma ci-dessus en précisant à chaque fois le nom de l'interface ethX. Pour vous aider, vous pouvez consulter, sur la machine hôte, le fichier `demo/gw.topo` ce fichier détaille la configuration du réseau virtuel dans QemuNet. Puisque certaines machines ont plusieurs adresses IP, il vaut mieux systématiquement donner aux commandes des adresses IP, et non des noms de machines.
- Vérifiez avec 'ping' que les machines peuvent communiquer dans leurs réseaux locaux respectifs.
- Afficher les tables de routage avec la commande 'route -n'.
- Configurez les tables de routage des différentes machines à l'aide de la commande 'route'. Il faut également activer le relai des paquets sur `immortal` pour qu'il agisse comme un routeur. On rappelle quelques éléments de syntaxe dans le memento ci-dessous. Vérifiez avec ping que toutes les machines sont capables de communiquer

ensemble. Si ça ne passe pas, utilisez `tcpdump -n -i any` sur les différentes machines pour voir où ça coince.

- Faites un ping entre `opeth` et `grave`. Lancez `tcpdump -n -i any` sur `immortal` afin d'afficher le trafic qui circule...
- Si vous ne l'avez pas fait, simplifiez le routage en utilisant `default` plutôt que des routes explicites.

4.3 Routage Avancé

Voici une nouvelle configuration, composée de 4 sous-réseaux /24 dans le réseau 147.210.0.0/16 :



Démarrez ce réseau virtuel :

```
/net/ens/qemunet/qemunet.sh -x -s /net/ens/qemunet/demo/chain0.tgz
```

Les adresses IP sont déjà configurées. Il faut donc configurer les tables de routage afin que tout le monde puissent communiquer avec tout le monde. La machine `grave` nécessite l'utilisation de routes spécifiques, les autres peuvent utiliser des routes `default`

5 Bonus : Topologie réseau

Connectez-vous à la machine de votre voisin avec `ssh leNomDeLaMachine`. Lancez `ip neigh ls` pour afficher le cache ARP/NDP sur chacune des deux machines, constatez que chacune a une entrée pour le voisin.

Connectez-vous maintenant à `jaguar`, lancez `ip neigh ls`, pourquoi l'adresse MAC de votre machine n'y apparaît pas ?

Essayez de déterminer la topologie réseau. On a vu en cours que les machines de salle de TP avaient des adresses similaires. Déterminez comment sont regroupées les IPs serveurs (`bacchus`, `dns0`, `dns1`, `cocatrix`, `infini1`, `jaguar`, `mcgonagall`, `netapp`), pour faire un petit schéma du réseau. Observez les routes configurées sur les serveurs auxquels vous avez accès

ssh, contentez-vous d'observer l'adresse IP pour les autres. Qu'en déduire sur la topologie réseau ? Pourquoi est-il organisé ainsi ?