# TD séance 3 - USI orienté réseaux

L'objectif de ce TD machine est de se familiariser avec quelques concepts de base et des commandes utiles dans l'utilisation des réseaux.

## 1 À la découverte du réseau

### 1.1 Votre machine et celles de vos voisins

1. Dans un premier temps, regardez le résultat de la commande `ifconfig` (*man ifconfig*). Quelles informations cette commande vous permet-elle d'obtenir. A quoi servent-elles ?
2. Récupérez votre adresse MAC et votre adresse IP. À quoi correspondent ces deux adresses ?
3. Quelle est l'adresse du réseau ? Quelle est l'adresse de diffusion du réseau ?
4. Demandez à votre voisin son adresse IP et testez si sa machine est accessible par le réseau, à l'aide de la commande `ping`. Que se passerait-il si la machine était inaccessible ?
   Testez maintenant l'accessibilité de www.google.fr, puis faites le test sur l'ensemble des machines du réseau.

### 1.2 Routage

**Principe :** Le terme routage désigne le mécanisme qui consiste à déterminer le chemin par lequel les données sont acheminées jusqu'à leur destinataire à travers un réseau. Il est effectué au niveau 3 du modèle OSI.

1. La commande `route` permet d'afficher et de modifier la table de routage de la machine qui indique vers quelle interface envoyer les paquets en fonction de leur destination. Quelle est l'adresse de la passerelle vers un réseau externe.
2. La commande `traceroute` permet de connaître le chemin emprunté par les paquets IP pour aller d'une machine à une autre. Testez cette fonction pour différentes machines, interne et externe au réseau du département. Pouvez vous expliquer les résultats ?

## 2 Accès aux machines distantes

### 2.1 Connexion sur une machine distante.

Vous avez déjà vu qu'il est possible d'accéder à une machine distante et d'y effectuer des opérations grâce à `telnet`. Son successeur, `ssh`, permet de se connecter sur la machine distante avec un

niveau de sécurité plus élevé [1].

Utilisez la commande ssh pour vous connecter sur la machine *helicon* du département. Notez que vous retrouvez sur cette machine votre *home* tel que vous le connaissez, le serveur NFS [2] vous permettant d'avoir accès à votre arborescence de fichiers sur l'ensemble des machines du département. Les machines sont pourtant bel et bien distinctes, observez que les fichiers locaux aux machines sont différents. Vous pouvez par exemple comparer les contenus des répertoires `/tmp/` des deux machines.

## 2.2 Transfert de fichiers

En plus de se connecter sur une machine distante, il est utile de pourvoir transférer des données entre machine distante et machine locale.

1. Regardez le manuel de la commande `scp` (secure copy).
2. Depuis un terminal sur votre machine locale, transférez un de vos fichiers sur la machine *helicon* dans `/tmp/test_reseaux/`. Vérifiez que le fichier est bien présent dans ce répertoire.
3. Sur votre machine locale, créez un répertoire `tmp_reseau`, et transférez le répertoire `/tmp/TD_reseaux` dans celui-ci.

## 2.3 Ssh au quotidien

L'utilisation de `ssh` telle que vous l'avez utilisé jusqu'à présent peut se monter contraignante pour une utilisation récurrente (paramètres propres aux différentes machines et réseaux : login, passwd, adresse IP, nom de machine). Pour vous permettre d'utiliser plus simplement cet outil au quotidien nous allons voir comment configurer notre machine pour simplifier la connexion.

### 2.3.1 Création d'un fichier de configuration

S'il n'existe pas déjà, créez le répertoire `.ssh` à la racine de votre compte.

1. Observez le fichier `config` que vous avez récupérer précédemment. Quel est l'intérêt d'un tel fichier ? Essayez maintenant de créer votre propre fichier de configuration.
2. Le protocole `ssh` permet d'exporter un affichage X11 vers votre machine. Quelle option faut-il ajouter à la commande `ssh` ? Essayer d'ouvrir une fenêtre Emacs sur une machine distante.
3. Si vous vous connectez sur plusieurs machines en cascade, l'export de l'affichage ne suit pas. Il est possible de le faire suivre en incluant dans votre fichier de configuration une indication de forwarding. Trouver la directive appropriée à l'aide de `man 5 ssh_config`.

### 2.3.2 Génération et utilisation de clé ssh

Lors de la connexion sur une machine distante, ssh réclame son mot de passe à l'utilisateur. Pour éviter de redonner son mot de passe à chaque connexion, un utilisateur peut utiliser un couple de clés pour s'identifier sur le serveur.

[1] Le protocole réseau telnet transmet les communications en clair sur le réseau (entre autre login/passwd), tandis que le protocole ssh (Secure Shell) impose un échange de clés de chiffrement en début de connexion pour garantir des transferts de données chiffrées.

[2] Le système de fichiers NFS (Network File System) est un protocole qui permet à un ordinateur d'accéder à des fichiers via un réseau.

La création d'un couple de clés se fait grâce à la commande `ssh-keygen` et peut utiliser plusieurs méthodes de chiffrement grâce à l'option -t (rsa, dsa). Le couple généré se compose d'une clé publique (id_dsa.pub, id_rsa.pub) et d'une clé privée (id_dsa, id_rsa) présente dans le répertoire `.ssh`.

1. Générez un couple de clés en utilisant le mode de chiffrement dsa [3]
2. Sur la machine distante, copiez dans le fichier `~/.ssh/authorized_keys` le contenu de votre clé publique (attention, la ligne ne doit contenir aucun retour chariot).
3. Vérifiez que vous pouvez désormais vous connecter sans utiliser de mot de passe.

### 2.3.3 Mode paranoïaque

En tapant une passphrase pour protéger votre clé privée, vous augmentez la sécurité mais avez à donner un nouveau "mot de passe" à chaque connexion.

Pour éviter cela, il est possible d'utiliser un agent ssh qui va conserver dans un cache votre passphrase durant toute la durée de votre session sur la machine cliente. Sa mise en place consiste à :

- initialiser l'agent ssh : `eval 'ssh-agent'`
- ajouter votre passphrase dans le cache de l'agent : `ssh-add`.

Tester cette méthode en vous connectant sur la machine distante. Que se passe t-il si vous renouvelez l'opération depuis un autre terminal ?

[3] Pour ajouter un niveau de sécurité et protéger votre clé privée, il est possible de saisir lors de la création des clés une passphrase qui sera demandée à chaque connexion. Dans un premier temps, testez sans passphrase