

TP1

Le modèle en couches

L'objectif du TP est de vous faire découvrir le modèle en couches et de vous donner des outils pour travailler en réseau, notamment sur les serveurs de l'Université. Ce TP sera l'occasion de vous familiariser avec la ligne de commandes UNIX, que vous approfondirez en L3 informatique. Les commandes se tapent dans un *terminal*, en voici des particulièrement utiles:

- `ls` : liste les fichiers et dossiers du répertoire courant ;
- `mkdir test` : créer le répertoire *test* dans le répertoire courant ;
- `cd test` : vous permet de vous déplacer dans le répertoire *test* du répertoire courant. Le répertoire *test* devient le nouveau répertoire courant ; `cd ..` : permet de se placer dans le répertoire qui contient le répertoire courant ; `cd` : sans paramètre, permet de vous placez dans votre répertoire personnel, appelé *home directory* ou *home*.

Vous pouvez obtenir de l'aide à tout moment consultant le manuel à l'aide de la commande *man*, par exemple *man ls* affiche le manuel de la commande *ls*.

Je vous conseille également [*Pour aller plus loin avec la ligne de commande*](#), disponible gratuitement en version numérique.

1. SSH/SCP: Secure Shell/Secure CoPy

La commande *ssh* permet de lancer un terminal (shell) sécurisé (par cryptage des échanges) sur une machine distante. Le protocole SSH (couche application) définit les règles de communication. Pour en savoir plus sur la commande *ssh* lisez la page correspondante du manuel. Pour en savoir, plus sur le protocole SSH vous pouvez consulter les RFC (Request for comments) 4251, 4252, 4253 et 4254 ou l'article Wikipedia <http://fr.wikipedia.org/wiki/Ssh>.

1. Connectez-vous à *sirius* en *ssh*, essayez de lancer *konqueror*, puis déconnectez-vous.
2. Connectez-vous à *sirius* en *ssh* en activant le *X11 forwarding*. Cela signifie que l'application sera exécutée sur *sirius* mais se connectera au serveur X de votre machine pour l'affichage. Lancez *konqueror*, naviguez dans vos dossiers personnels et déconnectez-vous.
3. Lancez la commande *ls* via *ssh*.
4. Lancez uniquement l'application graphique *konqueror* via *ssh*.

La commande *scp* permet de copier des fichiers de façon sécurisée en s'appuyant sur SSH. N'hésitez pas à consulter la manuel.

5. Copiez un fichier sur *sirius* depuis votre poste.
6. Copiez un fichier depuis *sirius* dans votre *home directory*.

Le protocole SSH est sensible aux attaques de type *man in the Middle*. L'attaque consiste à se placer entre le client et le serveur et à se faire passer pour le serveur auprès du client et vice versa. Il est alors possible d'espionner la communication et donc de récupérer par exemple les mots de passe. Pour parer à ce genre de désagréments, le protocole SSH propose une authentification par clé public/privé (cryptage asymétrique).

7. Commencez par générer une paire de clés à l'aide de la commande *ssh-keygen*. **Attention! Il faut mettre un mot de passe à vos clés. Sinon il sera possible de se connecter au serveur en possédant juste votre clé privé!** Pour le TP, choisissez un mot de passe différent de votre compte sur *sirius* afin de pouvoir vérifier le bon fonctionnement de l'authentification par clé.

Les clés publiques autorisées à se connecter sont mises dans le fichier `~/.ssh/authorized_keys` (le signe `~` sert à désigner votre *home*). Il sera possible de se connecter à l'aide du mot de passe qui chiffre votre clé privée.

8. Gérer vos connexions à *sirius* de cette façon. Il faut passer votre clé privé en paramètre à *ssh*.

2. ARP: Address Resolution Protocol

Le protocole ARP se situe entre la couche 2 et 3 du modèle OSI vu en cours. Il définit comment relier une adresse IP (adresse du protocole Internet, couche 3 OSI: réseau) à une adresse MAC (*Media Access Control*, adresse matérielle, couche 2 OSI: lien). Le protocole ARP est « défini » dans la RFC 826 .

1. Cherchez et parcourez la RFC 826.
2. Déterminez l'adresse IP de votre machine sur le réseau des salles de TP :
3. Déterminez l'adresse MAC de la carte réseau qui vous connecte à ce réseau :
4. Comparez ces informations à celles d'un de vos voisins:
 - adresse IP :
 - adresse MAC :
5. Affichez la table ARP de votre machine. Comparez cette table avec celle de votre voisin.

La commande *ping* permet de tester l'accessibilité d'une machine sur un réseau IP par l'émission d'une requête ICMP *echo*. La machine peut répondre par une requête ICMP *echo reply* pour signifier sa présence. Cette commande est donc attachée à la couche 3 du modèle OSI.

6. Faites un « ping » sur la machine de votre voisin.
7. Affichez les tables ARP de vos machines, comparer aux résultats de la question 4 et expliquez.
8. Connectez-vous à *sirius* et consultez sa table ARP.

3. DNS: Domain Name Server

Il est plus pratique de retenir le *nom de domaine* d'une machine connectée à Internet que son adresse IP. Le protocole pour interroger un DNS (couche 7 OSI: applications) permet de relier un nom de domaine comme *google.fr* à une adresse IP (couche 3 OSI: réseau). L'interrogation d'un serveur DNS passe donc par la couche de transport (couche 4 du modèle OSI) et utilise le protocole de transport UDP. Les couches 5 et 6 du modèle OSI n'ont pas des sens ici, nous en reparlerons avec le modèle en couche TCP/IP.

1. Quelle est l'IP du DNS de votre poste de travail?
2. Quelle est l'IP du DNS sur *sirius*? Que contient le fichier */etc/resolv.conf*?
3. Utilisez les commandes *dig*, *nslookup* et *host* sur *google.fr*. Utilisez le manuel pour déterminer à quoi correspondent les informations retournées.

Pour en savoir plus sur les DNS, leur hiérarchie et bien plus encore:

http://en.wikipedia.org/wiki/Domain_Name_System, ainsi que les articles associés.

4. Le Web

Utiliser Firefox pour réaliser les opérations suivantes :

1. allez à la page du département informatique en tapant l'adresse dans la barre d'adresse, puis faites de cette page la page d'accueil de Firefox ;
2. dans un nouvel onglet, ouvrez la page du Wiki du département informatique <http://forge.in-fo.univ-angers.fr/wiki/> . Ajoutez cette page en favori ;
3. dans un nouvel onglet, allez à la page d'adresse IP 74.125.230.84 ;
4. ajoutez le moteur de recherche Wikipedia à la liste des moteurs disponibles dans la barre de re-

cherche de Firefox, puis cherchez « Web » dans Wikipedia à partir de cette barre de recherche. Ajoutez cette page en favoris dans un dossier nommé « réseaux ».

5. Accès aux ressources informatiques à distance

Afin d'accéder aux ressources informatiques du département à partir de chez soi (afin par exemple de continuer des TP de programmation à distance sans avoir à installer les compilateurs chez soi), plusieurs outils existent. Nous allons en explorer trois : le VPN du département, Putty et WinSCP.

5.1. VPN

Ouvrir une connexion VPN par <https://vpn.info.univ-angers.fr/>

Une fois la connexion ouverte :

1. envoyez un fichier sur son compte ;
2. téléchargez un fichier de son compte ;
3. ouvrez une session sur sirius par ssh ;
4. essayer de refaire ces manipulations en dehors de l'Université, c'est tout l'intérêt du VPN.

5.2. PuTTY (sous windows)

PuTTY est un client libre SSH/Telnet pour Windows et Unix.

1. Ouvrez une session sur *sirius* par SSH.
2. Ouvrez une session sur *sirius* par SSH avec l'authentification par clés.
3. Essayez d'ouvrir une application graphique (activez le *X11 forwarding*). Expliquez.

5.3. WinSCP (sous windows)

WinSCP est un client libre SFTP/SCP pour Windows utilisant SSH (il partage une partie de son code avec PuTTY). Il permet le transfert sécurisé de fichiers entre un client et un serveur SSH.

1. Ouvrez une session sur votre compte *sirius* par SSH.
2. Envoyez / téléchargez des fichiers sur votre compte.
3. Testez l'identification par clés.