

# TP Réseaux

Nicolas Prigent

Ce TP vous permettra de mettre en pratique certains des aspects du cours *Réseaux*. Nous utiliserons à cette fin plusieurs outils en ligne de commande. N'oubliez pas que vous pouvez à chaque instant demander des informations sur une commande du terminal sur Internet ou en tapant `man commande` sous Linux et `commande /?` sous MS-Windows.

## 1 Découverte de la configuration réseau

Nous allons commencer par observer la configuration réseau de notre machine en utilisant la commande `ifconfig` (pour InterFace CONFIGUlator) sous Linux ou `ipconfig` (pour Internet Protocol CONFIGUlator) sous MS-Windows. Ouvrez un terminal ou une commande MS-DOS et tapez la commande appropriée. Observez ce qui s'affiche. En vous basant le cours, qu'apprenez-vous ?

Nous allons maintenant nous intéresser à la table de routage de la machine locale. Pour ce faire, utilisez la commande `route` qui est disponible à la fois sous Linux et sous MS-Windows (même si les données affichées le sont sous une forme différente). Quelles sont les informations qui s'affichent ? Que signifient-elles ? Que pouvez-vous en déduire ?

## 2 Utilisation d'outils réseaux

Après avoir observé la machine locale, nous allons nous intéresser à sa connexion à l'Internet, et à sa possibilité d'atteindre les serveurs de Google. Pour cela, nous allons utiliser la commande `ping`. Cette commande permet d'utiliser le protocole *Internet Control Management Protocol* (ICMP) qui est un protocole de même niveau que UDP et TCP et fonctionne donc au dessus d'IP. La commande `ping machine` envoie un message ICMP Echo request à machine. Cette machine est alors supposée retourner un message ICMP Echo reply. La commande `ping` (identique sous Linux et MS-Windows) va notamment mesurer le temps mis par la communication pour faire l'aller-retour<sup>1</sup>, le `ttl` du paquet reçu, etc. Essayez maintenant de *pinguer* `www.google.com` et observez les résultats. Vous pouvez aussi tester la commande `ping` sur d'autres machines et comparer les résultats.

Comme nous pouvons le constater, la commande `ping` a transformé d'elle-même les noms d'hôtes en adresse IP. L'outil `nslookup` (lui aussi disponible

---

<sup>1</sup>Cette donnée est souvent abrégée RTT pour Round-Trip Time.

à la fois sous Linux et MS-Windows) permet d'interroger les DNS en ligne de commande. Essayez d'obtenir les adresses IP des sites `www.google.com` et `www.neekotech.fr`. Quelles différences apparaissent ? En sachant que l'un de ces deux domaine appartient à une multinationale qui utilise en fait de nombreux serveurs pour répondre à vos requêtes sur l'Internet, que pouvez vous déduire de ces réponses ?

Nous avons vu en cours que nos paquets traversent plusieurs routeurs avant d'atteindre leur destination. La commande `tracroute` (`tracert` sous MS-Windows) permet d'obtenir la liste des routeurs présents sur la route entre la source (c'est à dire notre machine) et la destination. Pour ce faire, `tracroute` se base sur le `ttl` des paquets IP. Rappelons que lorsque le `ttl` d'un paquet atteint 0, le routeur jette ce paquet. Il est alors censé prévenir la source de ce fait en envoyant un message ICMP `Exceeded`<sup>2</sup>. Essayez de trouver la route vers `www.neekotech.fr`, et vers d'autres serveurs de votre choix. Que constatez vous ?

### 3 Un logiciel de chat très simple en netcat

Netcat (commande `nc` sous MS-Windows<sup>3</sup> comme sous Linux) est un outil qui réalise les même fonctions que l'outil Unix `cat`, mais sur le réseau. Il est ainsi possible de lire et d'écrire dans un socket, de rediriger les informations venant du réseau dans un fichier, d'envoyer les informations d'un fichier via le réseau, etc.

Nous allons commencer par utiliser Netcat localement. Autrement dit, nous allons lancer deux fois Netcat sur la même machine, une fois en mode serveur, et une fois en mode client. Ouvrez deux terminaux ou deux commandes MS-DOS. Lancez dans une des fenêtre Netcat en mode serveur sur un port de votre choix. Ensuite, lancez Netcat en mode client dans l'autre fenêtre en lui demandant de se connecter au même port. Comme adresse IP, vous pouvez utiliser soit l'adresse que `ifconfig` vous a retournée, soit le nom de machine `localhost`<sup>4</sup>, soit l'adresse `127.0.0.1`<sup>5</sup>. Si la connexion réussit, le texte que vous tapez dans une des fenêtre sera envoyé par le réseau (même si c'est ici une communication locale) et s'affichera dans l'autre fenêtre.

Ceci fait, choisissez un binôme sur une autre machine et établissez un canal de chat entre vos deux machines.

---

<sup>2</sup>Ces messages ne sont parfois pas envoyés pour éviter des attaques ou préserver la confidentialité de l'architecture réseau. Ils peuvent aussi être filtrés par certains routeurs. Si trois étoiles apparaissent sur la ligne, cela signifie que les messages ICMP `Exceeded` n'ont pas été émis ou ont été filtrés. Dans tous les cas, l'expérience ne fonctionne pas, c'est ainsi.

<sup>3</sup>Netcat n'est pas disponible par défaut sous MS-Windows mais il peut être téléchargé à l'adresse <http://joncraton.org/blog/46/netcat-for-windows>. Comme il est parfois utilisé pour attaquer les réseaux, il est considéré par certains anti-virus comme un programme malveillant. Il n'en est rien.

<sup>4</sup>`localhost` est, par convention, le nom de la machine locale, quelle que soit cette machine.

<sup>5</sup>Dans le standard IP, `127.0.0.1` est l'adresse de la machine locale, quelle que soit sa ou ses autres adresses IP.

## 4 Communiquer avec un serveur web à l'aide de netcat

Le protocole `http` fonctionne en mode texte. Nous allons donc utiliser `netcat` pour communiquer avec le serveur `http://www.neekotech.fr`. En vous souvenant qu'un serveur `http` écoute sur le port `80` et en vous servant des informations de la page wikipedia `http://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol`, essayez de communiquer avec le serveur. Tentez de récupérer quelques pages, et éventuellement quelques fichiers. Essayez aussi de récupérer une page qui n'existe pas et observez la réaction du serveur.