université de BORDEAUX

TP1 - Commandes de Base

L'objectif de ce TP est de se familiariser avec un certain nombre de commandes et de fichiers de configuration qui permettent de sonder la configuration de votre machine et du réseau local. Ces commandes sont souvent assez verbeuses et il faut s'habituer à retrouver les informations qui nous intéressent. Ce TP nous permet également de voir comment sont concrètement déployés les différents protocoles vus en cours.

1 Interfaces réseau et Adresse IP

Les commandes `/sbin/ifconfig` et `ip addr ls` permettent de récupérer la configuration des différentes interfaces réseaux (carte Ethernet, carte Wifi, boucle locale, ...).

- Observez les interfaces `eth0` et `lo` de votre machine avec `/sbin/ifconfig`. Indiquez les adresses IPv4 (champ inet) et IPv6 (champs inet6) correspondantes, la taille de la partie réseau, les tailles maximales de paquets (MTU, Maximum Transmission Unit), etc. Utilisez également la commande `ip addr ls` , c'est la même chose, mais en version plus moderne.
- Pour les IPv4, utilisez `ipcalc l_adresse_ip/la_taille_du_prefixe` pour obtenir le détail des adresses appartenant au même réseau que celle de votre machine.
- L'interface `lo` désigne la boucle locale. Elle permet aux programmes tournant sur une même machine de se connecter les uns aux autres aussi, sans passer par le réseau physique externe. Regardez les adresses IPv4 et IPv6 de l'interface `lo` et comparez-les avec celles de la machine de votre voisin.
- Observez que la MTU n'est pas la même pour `lo` et pour `eth0`, pourquoi ?
- La commande `ping uneIP` permet de tester la connectivité IP par l'émission d'une requête echo ICMP. Vérifiez que vous êtes bien relié à la machine de votre voisin (utiliser control-c pour l'arrêter). Testez à la fois avec une IPv4 et avec une IPv6.

2 Netcat & Netstat

Netcat (via la commande `nc`), est un utilitaire en ligne de commande qui permet de lire et d'écrire des données à travers des connexions réseau en utilisant les protocoles TCP ou UDP. Nous allons utiliser cette commande pour lancer un serveur sur un port donné et connecter un client dessus.

Afin d'observer les connexions établies nous allons utiliser l'utilitaire `netstat`. Netstat (pour Network Statistics) est un outil en ligne de commande qui fournit des informations sur les connexions réseau (entrant et sortant), les tables de routage, les statistiques d'interface, ...

— Lancez `nc -l -p 12345` et laissez-le tourner . Observez (en passant par un autre terminal) dans `netstat -tuan` ou `ss -tuan` l'apparition du service parmi les autres. Note : utilisez `grep` pour retrouver plus facilement le port 12345.
— Ajoutez à netstat ou ss l'option `-p` pour constater que c'est bien le programme `nc` qui est à l'écoute. C'est donc un mini-serveur que l'on a lancé, auquel on va maintenant se connecter.
— Dites à votre voisin de lancer `nc votremachine 12345` , pour jouer le rôle du client. Observez dans `netstat -tun` ou `ss -tu` la connexion établie entre client et serveur.
— Tapez des lignes d'un côté ou de l'autre, observez que c'est effectivement transmis de l'autre côté.

3 Protocole ARP

Le protocole ARP (Address Resolution Protocol) est un protocole de réseau utilisé pour associer une adresse IP (Internet Protocol) à une adresse MAC (Media Access Control) sur un réseau local.

Une table (ou cache) ARP est une table de correspondance qui stocke les associations entre les adresses IP et les adresses MAC des appareils sur un réseau local (LAN). Elle est maintenue par chaque appareil connecté au réseau (comme les ordinateurs, routeurs, et commutateurs) pour permettre une communication efficace au sein du réseau.

A l'aide de la commande `arp` nous allons interroger et manipuler la table ARP de notre machine.

— Identifiez les adresses des machines voisines avec lesquelles des échanges récents ont eu lieu (table ARP, disponible par la commande `/usr/sbin/arp` , on peut utiliser l'option `-n` pour avoir les adresses IP plutôt que les noms de machines). Il doit y avoir au moins l'adresse du routeur (en `.254`, on verra dans la section routage ci-dessous).
— Vérifiez que lorsque vous émettez avec `ping -4` une requête ICMP echo vers une machine de la salle qui ne figure pas encore dans votre table ARP, cette machine apparaît dans la table ARP de votre machine et la vôtre, dans la table ARP de l'autre.
— Essayez la commande `ip neigh ls` ; c'est la même chose en version plus moderne, et contient notamment aussi les voisins en IPv6.
— Essayez de faire un ping vers `8.8.8.8` et vers `10.0.230.6` . Pourquoi leurs adresses n'apparaissent pas dans la table ARP ?

4 Résolution de noms (DNS)

Le DNS (Domain Name System) est un service qui traduit les noms de domaine lisibles par l'homme (comme www.u-bordeaux.fr) en adresses IP numériques que les ordinateurs utilisent pour communiquer sur un réseau. Il fonctionne comme un annuaire téléphonique de l'Internet, permettant aux utilisateurs d'accéder aux sites web et autres services en utilisant des noms faciles à retenir.

Nous allons voir dans cet exercice, comment le machines du CREMI sont configurées pour accéder à ce service et comment utiliser directement ce service à l'aide de commandes.

— Lisez le fichier `/etc/resolv.conf` et `man resolv.conf`, à quoi correspond cette adresse IP ?
La ligne `search` permet d'éviter d'avoir à taper le nom de machine en entier. Essayez de taper `http://www/` tout court dans un navigateur web et observez comment cela est complété pour confirmer.

— Pour effectuer explicitement une résolution de nom, utilisez la commande `host` (ou éventuellement `nslookup`).

— Essayez de résoudre `yahoo.com` . Pourquoi y a-t-il plusieurs adresses IP ?
Observez également que cela retourne à la fois des adresses IPv4 et des adresses IPv6. Réessayez plusieurs fois. Il peut arriver que le résultat soit différent, pourquoi ?

— Parfois il est aussi utile d'ajouter des noms de machine à la main, jetez un œil au fichier `/etc/hosts` (et au manuel). Remarquez dans `/etc/nsswitch.conf` la ligne `hosts:` qui indique que c'est le fichier `/etc/hosts` (`files`) qui a la priorité sur la résolution DNS (`dns`).

5 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 (ligne `host`) ? Observez les adresses IP de ces serveurs.

— Trouvez le numéro de port de ce service, vérifiez dans `/etc/services`, retrouvez-y également les ports `http`, `ssh`, `x11`, etc. (utilisez grep !)

— Vos fichiers sont stockés sur un serveur NFS, utilisez la commande `df ~` pour repérer le nom du serveur, le chemin sur le serveur, et le chemin où cela apparaît sur votre machine.