

Le TP donnera lieu à la rédaction d'un rapport pdf contenant des captures d'écran de votre travail ainsi que votre analyse/discussion pour les différentes questions. Le travail doit être organisé en équipes de deux étudiants (binôme), et vous devez produire un rapport contenant pour chaque question : une description de l'expérience, ligne de commande + sortie écran et analyse. Votre rapport doit être rendu **au plus tard 5 jours après la séance du TP**. Chaque membre de l'équipe doit faire toutes les étapes d'installation, de configuration et les expériences séparément sur sa machine, le travail d'équipe est réservé à la partie analyse où vous devez échanger, discuter, et produire une réponse commune.

Veuillez classer les réponses par numéro. Le fichier portera votre **nom** suivi du numéro du TP en l'occurrence ici TP2, exemple: **martinTP2.pdf**
Le fichier sera envoyé à asma.berriri@universite-paris-saclay.fr

TP 2

Dans ce TP, nous allons configurer un réseau simple en utilisant deux machines virtuelles et analyser le trafic TCP et UDP afin de comprendre les différentes fonctionnalités.

Nous avons besoin pour ce TP, de deux machines virtuelles Linux. Si vous n'avez pas encore installé les machines, suivez les étapes ci-dessous :

- Installez Virtualbox sur votre machine physique : <https://www.virtualbox.org/>
- Télécharger Linux Ubuntu 20.04 en fichier image ISO : <https://ubuntu.com/download/desktop>
- Créer une nouvelle machine virtuelle sur Virtual box : "Machine → new" avec au moins 2 Go de RAM et 25 Go d'espace de stockage sur un disque dur de type VDI.
- Vous pouvez toujours modifier les paramètres après la création dans l'onglet "Paramètres".
- Installer Ubuntu sur la machine virtuelle créée : "Setting → storage → add optical drive" puis ajouter l'image téléchargée, démarrer la machine et suivre les instructions d'installation.
 - o Faites attention à sélectionner "installer" et non "essayer"
 - o **Important** : N'oubliez pas de définir un mot de passe pour l'utilisateur root.

Partie 1 - Configuration du réseau

Avant de démarrer les **deux** machines virtuelles, créez une nouvelle interface réseau : " Setting → Network → adapter 2 → activate interface " puis, configurez l'accès réseau en *interne* **uniquement pour l'adaptateur 2** : " Setting → Network → Network access → Internal ". Cette configuration permet de connecter les deux machines, toutes les configurations pendant le TP doivent se faire sur cette interface. La première interface qui doit rester sur NAT est utilisée uniquement pour accéder à internet, ne changez pas sa configuration pendant le TP.

1. Démarrez les **deux** machines et configurez les interfaces réseau. La manipulation des interfaces réseau se fait à l'aide de la commande ifconfig. Pour obtenir des informations sur toutes les interfaces disponibles sur le système :

```
> ifconfig -a
```

Sans l'option -a, la commande n'affiche que les interfaces qui sont actuellement actives.
Vous pouvez activer/désactiver une interface en utilisant les commandes :

```
> ifup [interface]
> ifconfig [interface] up
> ifdown [interface]
> ifconfig [interface] down
```

Voici une commande typique pour configurer une interface :

```
> ifconfig "interface_name" 192.168.10.5 netmask 255.255.255.0
```

Note :

Si le masque n'est pas spécifié, il est calculé en fonction de la classe de l'adresse.

Une entrée correspondant au réseau associé à l'interface est automatiquement ajoutée à la table de routage.

2. Testez la connectivité entre les deux machines en utilisant la commande *ping* dans les deux directions :

```
> ping "adresse_destination"
```

Partie 2 - Analyse du trafic TCP et UDP

Utilitaires :

- **tsock** : générateur de trafic TCP ou UDP : **disponible dans l'archive zip fourni**
- **tcpdump** : outil permettant de capturer le trafic circulant sur le réseau

Avis et manuel disponibles :

- Guide d'utilisation de *tsock* (*fourni dans l'archive aussi*)
- Instructions pour l'utilisation de *tcpdump*
- Commande *man*

Utilisation du programme tsock

1. Effectuez un échange de données entre un tsock source (sur une première machine Linux) et un tsock puits/récepteur (sur l'autre machine Linux), via UDP puis TCP, en utilisant un numéro de port de votre choix entre 5000 et 9000.

Dans les deux cas, lancez le programme *tsock* puits avant le programme *tsock* source.

- a. Est-ce que vous voyez de séquençage en utilisant UDP, en utilisant TCP ?
 - b. Constatez-vous des pertes en utilisant UDP, en utilisant TCP ?
 - c. Proposez et réalisez une expérience qui met en évidence le manque de fiabilité du service offert par UDP (vous pouvez utiliser les options `-l ##`, `-n ##` et si nécessaire `-w` sur la Source).
2. Répétez la question 1 en exécutant cette fois la source tsock **avant** le puits tsock.
 - a. Qu'observez-vous en utilisant UDP, en utilisant TCP ?
 - b. Pour UDP, vérifiez si les données transmises sont reçues par le programme *tsock* puits. Pensez-vous que le comportement de UDP est acceptable par rapport au service qu'il offre ?

Utilisation du programme tcpdump

3. Répétez l'expérience de la question 1 et capturez (via tcpdump) le trafic correspondant en filtrant le numéro de port utilisé par le sink :

Lancez tcpdump **dans un autre terminal** sur la machine Source ou la machine Puits comme suit :

```
> sudo tcpdump port "port" -i "interface_name"
```

où "port" désigne le numéro du port utilisé par le lien.

- a. Montrez que UDP est un protocole sans connexion.
 - b. Mettez en évidence que le protocole TCP est un protocole orienté connexion. Retrouvez les phases d'établissement de la connexion, de transfert et de fermeture de la connexion.
 - c. Analysez la phase de transfert de données de TCP et mettez en évidence (par le biais d'une expérience) les causes qui font que TCP ne conserve pas la même frontière de messages envoyés.
4. Répétez l'expérience de la question 1 (en UDP ou TCP) et capturez le trafic correspondant (filtrez sur le numéro de port utilisé par le Sink), en visualisant cette fois le contenu des trames **Ethernet** capturées à l'aide de l'option -e.

Pour ce faire, vous devez utiliser la commande :

```
> sudo tcpdump port "port" -i "interface_name" -e
```

où "port" désigne le numéro du port utilisé par le lien.

En s'appuyant sur le format des en-têtes Ethernet, IP, UDP et TCP présenté dans le cours, Déterminer :

- a. les adresses MAC et IP des machines source et destination ;
 - b. l'information indiquant que la trame transporte UDP ou TCP ;
 - c. le numéro du port utilisé par le puits ;
 - d. le numéro de port utilisé par le programme source, d'où vient-il ?
5. Jusqu'à présent, vous n'avez effectué que des transferts d'une machine à une autre (transfert unicast).
 - a. Rappelez ce qu'on appelle un transfert en mode "broadcast".
 - b. À l'aide de la commande `> tcpdump -xx broadcast`, déterminez expérimentalement l'adresse de diffusion du réseau.