Réseaux pour ingénieurs
GLO-2000

TP2 : Transmission de paquets

Professeur responsable :
Ronald Beaubrun
Ronald.Beaubrun@ift.ulaval.ca

Responsables des travaux pratiques :
Pierre Wendling et Vincent Primpied
GLO2000.laboratoires@gmail.com

Université Laval
Faculté des sciences et de génie
Automne 2022

Ce deuxième TP a pour but de vous familiariser avec des outils de création de paquets et de communication réseau, et de comprendre des aspects pratiques en lien avec les **couches réseau et transport**. Pour réaliser ce travail, vous devrez utiliser les outils Wireshark, Nping et Ncat.

Modalités de remise

- À faire en équipe de 3.
- Le rapport doit être rédigé au complet sur un logiciel de traitement de texte ou en LaTeX et rendu au format PDF (une pénalité de 5% sera attribuée pour format incorrect, remise de photographie ou de scan).
- Les fichiers à remettre sont :
  - Le fichier `TP2.pdf`, contenant les réponses textuelles.
  - Les fichier `TP2_<numéro de question>.pcapng`, contenant les paquets capturés.
  - Les fichiers sont à rendre dans une unique archive zip avec l'organisation suivante :

```
TP2_equipe_<votre numéro d'équipe>.zip
 ├── TP2.pdf
 ├── TP2_Q1A.pcapng
 ├── ...
 ├── TP2_Q4A_TCP.pcapng
...
```

  N. B. : Une pénalité de 5% sera appliquée pour chaque point non respecté.
- Remise uniquement via le portail des cours.
- Date limite de remise est la suivante : **12 octobre 2022 à 23h00 (fuseau horaire de Québec)**.
- Tout travail remis en retard se verra attribuer la note **0**.

1 Nping (5 points)

1. À l'aide du logiciel Nping, créez les paquets décrits ci-dessous et interceptez-les en utilisant Wireshark. Pour chaque paquet, vous devez donner **la ligne de commande utilisée pour le créer** ainsi que **la trace réseau capturée** avec Wireshark. Si votre capture contient des paquets non-pertinents, vous serez pénalisés. La résolution de nom (DNS) ne doit pas être incluse.

   (a) Créez le paquet suivant et imprimez la trace dans le fichier TP2_Q1A.
   - Adresse de destination : www.kernel.org
   - Protocole : TCP
   - Port source : 10628
   - Port de destination : 80
   - *Flag* : SYN
   - Nombre de paquets : 1

(b) Créez le paquet suivant et imprimez la trace dans le fichier TP2_Q1B.
- Adresse de destination : www.gnu.org
- Protocole : TCP
- Port source : 10928
- Port de destination : 443
- *Flag* : SYN
- Nombre de paquets : 1

(c) Créez le paquet suivant et imprimez la trace dans le fichier TP2_Q1C.
- Adresse de destination : www.freebsd.org
- Protocole : TCP
- Port source : 13674
- Port de destination : 80
- *Flag* : ACK
- Nombre de paquets : 2

2. Générez un paquet avec la commande suivante :

```
nping www.doomwiki.org --ether-type=0x0806 --udp -p80 -g443 --flags 0x18 -c 1
↪  --ttl 32
```

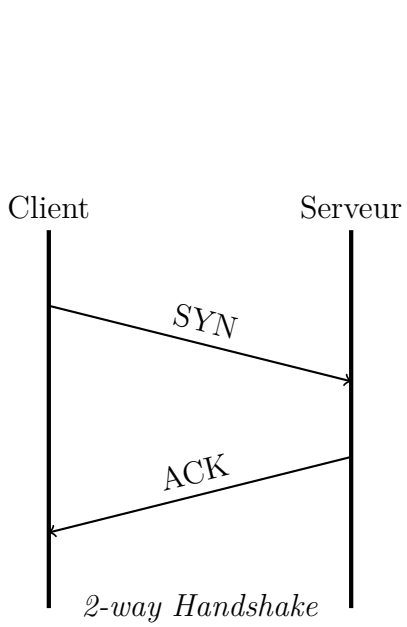
Donnez deux raisons pour lesquelles vous ne recevez pas de réponse de la part de www.doomwiki.org.

2 Programme mystère (4 points)

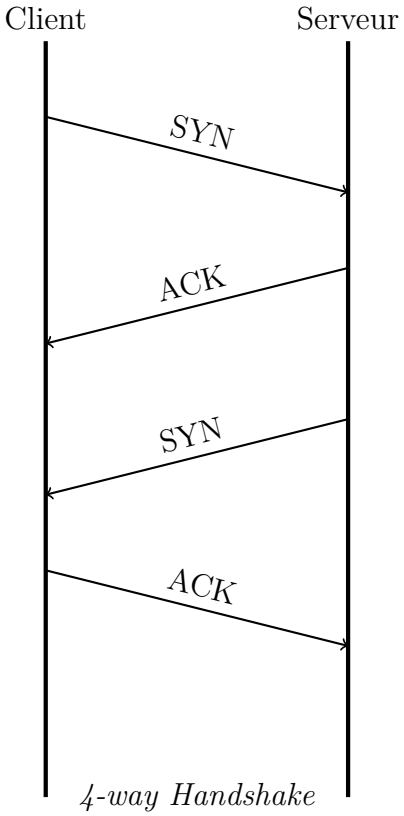
La trace TP2-Q2.pcapng contient plusieurs paquets produits à la suite de l'exécution d'un programme utilitaire particulier. En analysant ces paquets, déduisez **quel programme** a été exécuté puis donnez-en l'**utilité** et le **fonctionnement**. Indice : regardez les TTL.

3 *3-way Handshake* (3 points)

Soient les méthodes de connexion *2-way Handshake* et *4-way Handshake* représentées ci-dessous.



2-way Handshake



4-way Handshake

Donnez leurs désavantages respectifs par rapport à la méthode standard *3-Way Handshake*.

4 Ncat (3 points)

1. À l'aide du logiciel Ncat, établissez une connexion sur le port 3892 de votre machine en utilisant deux terminaux et transmettez le message : `Hello World`
   Effectuez cette communication en mode TCP (mode par défaut) puis en mode UDP (ajouter `-u` côté serveur et client). Pour chacun des modes, interceptez la communication avec Wireshark.
   — Expliquez pourquoi le nombre de paquets généré n'est pas le même selon le mode.
   — Remettez tous les paquets pertinents dans les traces :
   — *TP2_Q4A_TCP.pcapng* pour le mode TCP ;
   — *TP2_Q4A_UDP.pcapng* pour le mode UDP.
2. Démarrez un serveur Ncat en mode UDP et écoutant sur le port 31737. Avec un autre terminal, d'**une seule commande Nping**, envoyez 2 paquets UDP transmettant le message 'GLO-2000'. Assurez-vous qu'à la suite de la communication le serveur affiche bien 2 fois le message 'GLO-2000'.
   Donnez la commande Ncat pour démarrer le serveur et la commande Nping pour communiquer avec le serveur. Remettez également la trace de la communication dans un fichier *TP2_Q4B.pcap*.