



Réseaux pour ingénieurs GLO-2000

TP2 : Transmission de paquets

Professeur responsable:

Ronald Beaubrun

Ronald.Beaubrun@ift.ulaval.ca

Responsables des travaux pratiques:

Louis Fortier-Dubois et Jean-Alexandre Beaumont

glo2000a17@gmail.com

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 2 ou 3.
- Le travail doit contenir vos noms et vos numéros d'étudiant.
- Le type de fichier remis doit être un PDF (une pénalité de 10% sera attribuée dans le cas contraire).
- Nom du fichier à remettre: TP2-numero_d_etudiant_d_un_des_membres.pdf
- Remettre sur le portail des cours.
- Date limite : 18 octobre 2017
- 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.

(a) Créez le paquet suivant et imprimez la trace réseau.

- Adresse de destination: `www.cisco.com`
- Protocole: TCP
- Port source: 1337
- Port de destination: 80
- Flag: SYN
- Nombre de paquets: 1

(b) Créez le paquet suivant et imprimez la trace réseau.

- Adresse de destination: `www.wikipedia.org`
- Protocole: UDP
- Port source: 9999
- Port de destination: 80
- Nombre de paquets: 1

(c) Créez le paquet suivant et imprimez la trace réseau.

- Adresse de destination: `www.imdb.com`
- Protocole: TCP
- Port source: 11111
- Port de destination: 80
- Flag: RST
- Nombre de paquets: 1

2. Générez un paquet avec la commande suivante :

```
nping www.google.com --tcp -g 1337 -p 2000 -c 1 -S 111.111.111.111 --ttl 2
```

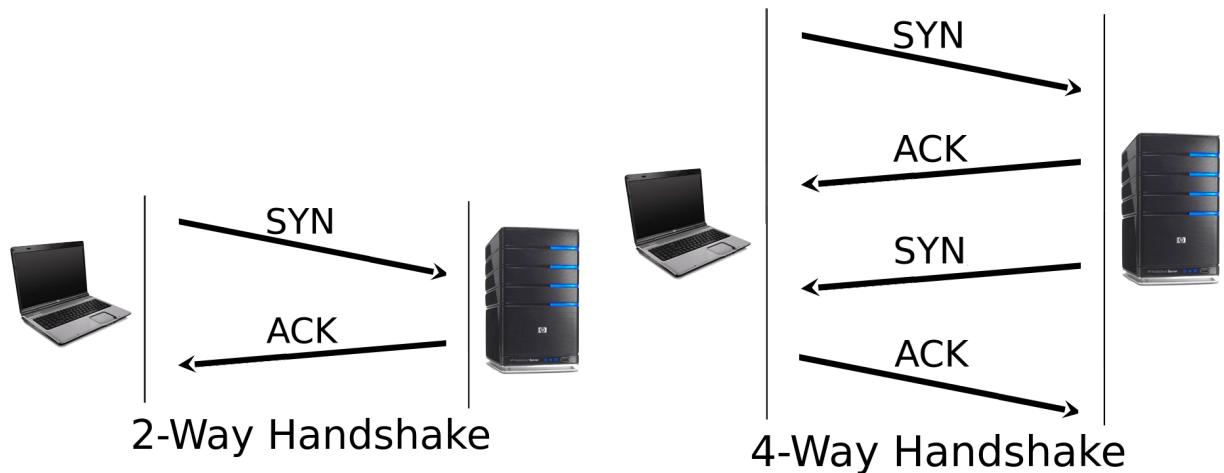
Donnez trois raisons pour lesquelles vous ne recevez pas de réponse de `www.google.com`.

2 Programme mystère (4 points)

La trace TP2-Q2.cap 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 et les ports de destination des paquets.

3 3-way handshake (3 points)

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



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 votre machine en utilisant deux terminaux et transmettez le message :

I'd tell you a joke about UDP, but you might not get it and I won't even care.

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 : ceux générés en mode TCP dans un fichier *TP2-Q4a-TCP.cap* et ceux générés en mode UDP dans un fichier *TP2-Q4a-UDP.cap*.
2. Démarrez un serveur Ncat en mode UDP et écoutant sur le port 1337. Avec un autre terminal, d'**une seule commande Nping**, envoyez 5 paquets UDP transmettant le message « bonjour ». Assurez-vous qu'à la suite de la communication le serveur affiche bien 5 fois le mot bonjour. 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.cap*.