TELECOM Nancy 1A - RS -Réseaux
TP2 Couche Transport

1 TCP : aspects protocolaires

Exercice 1 Capturer avec Wireshark un flux TCP simple, par exemple en tapant dans la console :

```
wget http://www.videolan.org
```

Dans Wireshark, inspecter le flux TCP lié a cette requête. Pour cela, trouver un des messages du flux TCP, le sélectionner et faire clic droit -> suivre flux TCP. Un filtre isole alors ce flux spécifique du reste des paquets capturés pour plus de lisibilité.

Nous allons nous intéresser ici à l'en tête TCP. Considérons **le premier segment**.

- Quels sont les numéros de ports source et destination ?
- Quelle est la taille du premier segment ? Pourquoi ?
- Quelle est la valeur du numéro de segment absolue et relative ?
- Quelle est la valeur du numéro d'acquittement absolue et relative ? Même question pour le second segment.
- Quelle est la taille de l'en-tête TCP ?
- Quel Flag est positionné pour ce segment ?
- Quelle est la taille de la fenêtre récepteur ? À quoi cela correspond-il ?
- Quelles options de TCP sont déclarées possibles pour cette connexion ?

Ouverture et fermeture de connexion :

- Par un schéma, indiquer les échanges réalisés lors de l'ouverture de connexion (4 premiers messages). Préciser les flags et les numéros de séquence relatifs et d'acquittement.
- Même question avec la fermeture de connexion et les 4 derniers messages.

2 TCP : contrôle de flux

Préambule : pour se rapprocher des caractéristiques d'un lien réel et non simulé in silico, configurer les liens entre le switch et les machines avec les propriétés suivantes (pour chaque lien et dans les deux sens) :

- Delay : 5ms
- Bandwidth : 2 000 KB/s
- MTU : 1500 bytes [1]

Exercice 2 **iperf** est un utilitaire permettant d'évaluer la capacité d'un réseau en générant du trafic synthétique. Il fonctionne sur un modèle client / serveur. Dans votre topologie du cyber-range :

- Exécuter iperf sur vos machines tout en capturant le trafic généré le switch ou sur une des machines terminales :
  - exécuter sur le serveur : iperf -s
  - exécuter sur le client : iperf -c @IP_serveur -n 5M
- Mesurer la taille de la fenêtre d'émission en début de transmission (somme de la taille des données envoyées sans acquittement).

1. Cette contrainte ne semble pas bien pris en compte par le cyber-range actuellement

— Étant donnée la formule : Throughput = taille_fenêtre/RTT bytes/s, et sachant que le RTT simulé est de 20ms, en déduire le débit initial.

— Mesurer le temps entre l'envoi de deux acquittements successifs à la fin de la transmission. Remarquez comme l'envoi de segments et la réception d'ack est alternée. En déduire le débit sachant qu'en régime de croisière la réception d'un acquittement déclenche l'envoi d'un segment.

— Que signifie "Seq=1" sur les segments dans le sens client -> serveur tout au long de la transmission ?

3 TCP : pertes et retransmissions

Exercice 3 Pour provoquer des pertes et retransmissions, nous allons maintenant rajouter un taux de perte de 1% sur le lien entre le serveur et le switch dans le sens serveur -> switch.

— Vérifier que les segments perdus sont bien retransmis. Remarquez au passage qu'1% de pertes réduit le débit bien davantage que de 1% (car les pertes sont interprétées par TCP comme de la congestion et non comme un lien défaillant).

— Mesurer le temps entre un l'émission d'un segment perdu et sa retransmission. Ce temps est-il optimal (i.e. proche du RTT) ?