

TD3 : Internet Protocol Correction

Objectifs :

- Comprendre la limite de débit d'une connexion TCP
- Pouvoir corriger le dysfonctionnement d'un réseau
- Concevoir une application qui donne les sauts d'Internet (Traceroute)

Partie I : Débit théorique d'une connexion TCP

1.1 Dans une connexion TCP, comment appelle-t-on le temps mis pour recevoir l'acquittement d'un segment ? Cette valeur est-elle toujours constante ? Pourquoi ?

Round Trip Time = temps entre le début de l'émission d'un segment et la réception de l'ACK correspond.

Ce temps est variable car il dépend de nombreux facteurs :

- Le chemin dans Internet n'est pas fixe, le délai de propagation peut donc changer.
- L'état des réseaux traversés, les temps de traitements et les délais d'attente dans les buffers peuvent varier.
- L'accès au réseau peut être plus ou moins long en fonction de la méthode d'accès et de l'occupation du réseau
- Impact sur le débit des réseaux des communications des autres utilisateurs
- ...

1.2 Combien de segments au maximum peut-on envoyer au cours de ce temps ?

Puisque le RTT est le temps pour recevoir l'ACK du segment émis, pendant ce temps, l'émetteur peut envoyer au maximum la taille de sa fenêtre d'émission. En effet au-delà de cette valeur, il doit attendre un ACK pour émettre un autre segment. (c'est la définition de la taille de la fenêtre d'émission).

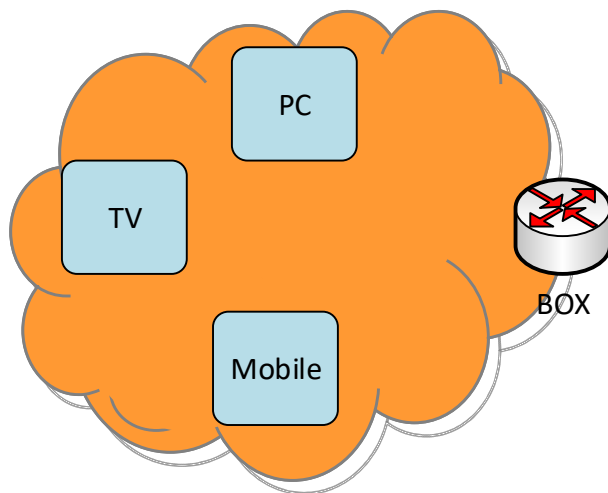
Cette valeur, la taille utilisable pour l'émission, est fixée par le récepteur via awnd.

1.3 En déduire une expression du débit maximum théorique d'une connexion TCP

Ainsi, pendant 1 RTT on peut envoyer awnd octets ce qui nous donne un débit maximal théorique de :

$$D_{max} = \frac{awnd \times 8}{RTT}$$

Partie II : Docteur réseau !



Réseau privé

Le réseau privé ci à côté propose 3 équipements utilisateurs (UEs) et une box (un modem/routeur). La technologie utilisée est du wifi pour les 3 UEs. La box a l'adresse 80.0.1.102 configurée en point à point avec le routeur du FAI 80.0.1.1.

1.1 Problème 1: accès à Internet

Une fois configuré le réseau ne fonctionne pas correctement. Les UEs peuvent communiquer entre eux et avec la box, en revanche, ils ne peuvent pas accéder à Internet alors que la box en est capable.

- a) Le problème d'accès à Internet peut-il venir de la table de routage de la box ? Pourquoi ?

La Box a accès à Internet comme aux UEs, c'est donc que sa table de routage est correcte.

- b) Que doit-on vérifier au niveau des UEs pour que ces derniers puissent accéder à Internet ?

Il faut vérifier que la configuration de la table de routage des UEs soient correctes : il est nécessaire d'avoir une route par défaut qui passe par la box, avec l'adresse de cette dernière dans le réseau privé comme adresse de passerelle.

- c) Le problème ne semble pas venir des UEs. Lister au moins deux problèmes que l'on peut rencontrer au niveau de la box et donner une solution pour les résoudre.
- Le routage n'est pas activé sur la box (sur Linux = mode `ip_forwarding`) du coup, quand un datagramme provenant d'un UE arrive sur la box alors qu'il n'est pas destiné à celle-ci, la box le supprime.
 - Le réseau domestique utilise un adressage privé. Or ce dernier n'est pas routable sur Internet. Il faut donc mettre en place du SNAT ou de la masquerade sur la box, transformant ainsi les adresses sources des messages par l'adresse publique de la box, 80.1.0.102. (S'il s'agit d'une machine Linux on peut utiliser iptables pour mettre ça en place en partant du principe que l'interface de sortie vers Internet est nommée `internet` : `iptables -t nat -A POSTROUTING -o internet -j MASQUERADE`)

1.2 Problème 2 : serveur web

On s'intéresse à la mise en place d'un serveur web sur le PC. On constate rapidement que le mobile peut consulter le serveur web avec son adresse privée, tout comme la télévision ou encore la box. En revanche aucune machine de l'extérieur ne peut le contacter.

- a) Quelle adresse est enregistrée dans le DNS pour ce serveur web ?

Avec l'adresse privée du serveur, les autres UEs du réseau domestique peuvent atteindre le serveur web.

NB : Vous pourrez trouver le sujet du TD sur Moodle

En revanche pour accéder d'Internet au serveur web, il faut une adresse publique. Du coup si l'on renseigne dans le DNS l'adresse privée, cela ne fonctionnera pas. Il faut donc renseigner l'adresse publique de la box : 80.0.1.102

b) D'où vient alors le problème ? Proposer une solution pour le résoudre.

Malheureusement, la box n'est pas le serveur web mais c'est elle qui reçoit des requêtes web avec elle-même comme destination.

Une solution est alors de rediriger les requêtes reçues par la box sur le bon équipement du réseau privé. Ici une solution possible est de changer la destination du datagramme avant le message. C'est ce que l'on nomme du DNAT (il est aussi possible d'utiliser des solutions de reverse proxy web par exemple). Avec de l'iptables en disant que le serveur web à l'adresse ip 192.168.0.32, cela donne la règle suivante :

```
iptables -t nat -A PREROUTING -d 80.0.1.102 -p tcp -dport 80 -j SNAT --to 192.168.0.32
```

Partie III : Traceroute

L'objectif de traceroute est d'obtenir les différents routeurs traversés par votre message jusqu'à sa destination. Contrairement à une application classique, client/serveur, traceroute ne fonctionne qu'avec un client : elle est asymétrique. Alors, une question se pose d'elle-même : comment traceroute fait-il pour avoir une réponse des routeurs sur son chemin et de la destination ?

3.1 *Pourquoi n'est-il pas question de faire un mode client-serveur pour faire fonctionner traceroute ?*

Si l'on voulait faire un mode client/serveur à l'application traceroute, il faudrait que tous les routeurs d'Internet installe l'application en mode serveur pour répondre aux requêtes des clients. Cela a un coût de déploiement comme de mémoire et de traitement pour les routeurs. On veut une information mais on ne veut pas installer de nouveautés sur les routeurs.

3.2 *Que fait un routeur quand il ne peut pas faire suivre un paquet IP ? Informe t'il quelqu'un ? Comment ?*

Lorsqu'un paquet IP ne peut pas atteindre sa destination, le routeur peut en informer la source avec un message ICMP. Cela peut aussi être désactivé ou plus vraisemblablement filtrer sur certains réseaux.

3.3 *Lister les différents cas pour lesquels un paquet ne pourrait pas être routé par un routeur. Parmi eux, lequel pourrait servir traceroute pour détecter les différents routeurs sur le chemin. Justifier.*

Plusieurs cas d'impossibilité de routage :

- Pas de route pour la destination, impossible à savoir
- MTU trop petite du prochain saut, difficile à utiliser pour tracer le chemin
- Header invalide (checksum erroné), faux au premier routeur rencontré
- TTL décrémenté à zéro par le routeur
- ...

Si les premiers sont difficiles à utiliser pour tracer un message, le TTL trop court est une bonne solution. Il suffit d'envoyer des messages avec un TTL croissant en partant de 1 pour recevoir les réponses successives des différents routeurs sur le chemin. C'est le message Time Exceeded.

NB : Vous pourrez trouver le sujet du TD sur Moodle

Il existe plusieurs modes dans traceroute, on considérera ici le mode UDP.

3.4 *Comment traceroute utilise cela pour tracer le chemin ?*

Il suffit d'envoyer des messages avec un TTL croissant en partant de 1 pour recevoir les réponses successives des différents routeurs sur le chemin. C'est le message Time Exceeded qui va apporter en retour l'adresse du routeur rencontré.

On envoie un message avec un TTL de 1, la réponse est le routeur à 1 saut, puis à 2, etc...

3.5 *Pourquoi traceroute a-t-il besoin de différencier les paquets émis ? Pourquoi ne pas utiliser un champ applicatif pour cela ? Comment fait-il alors ?*

Malheureusement si l'on doit faire ça au fur et à mesure, cela peut prendre beaucoup de temps, du coup il serait bien d'en envoyer plusieurs en même temps. Malheureusement certains paquets peuvent être filtrés, d'autres traités et revenir plus tard, d'autres prendre un second chemin (ce qui reste un pb). Il faut pouvoir être capable de savoir quel paquet a engendré le message retour icmp. Or ICMP ne recopie qu'au minimum 28 octet du paquet IP qui pose problème (et donc par forcément un champ applicatif).

On pourrait utiliser un morceau de l'en-tête IP non utilisé comme le TOS, mais certains FAI l'utilisent. Une autre solution est d'utiliser un champ de l'en-tête UDP qui ne sert pas ici, comme les numéros de port, pour avoir une numérotation des messages de traceroute. Ils seront ainsi recopiés dans le retour ICMP (20 octets Header IP + 8 octets UDP)