Internet - TD 2 : TCP et la MTU

> Objectif : comprendre la gestion de la MTU dans TCP/IP.

Exercice 1 : TCP et la fragmentation IP

> Un routeur peut être amené à fragmenter des paquets IP trop gros pour être transmis directement sur une laison dont la MTU est trop faible. Cette fragmentation doit être évitée dans la mesure du possible.

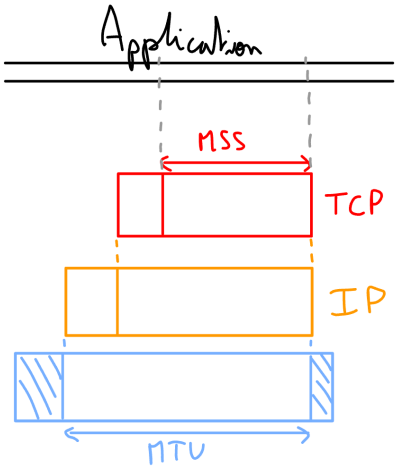
1. Pourquoi ce phénomène de fragmentation est-il indésirable ? Pourquoi a-t-il pourtant été spécifié et implanté dans la pile IP ?

Fragmenter = effort supplémentaire -> utiliser des ressources.
Perte de temps -> congestion
Le plus gros problème c'est de réassembler des fragments. Il faut donc un buffer pour garder en mémoire les fragments. Et que se passe-t-il si on a perdu un fragment ? En outre, combien de temps garder les buffers en mémoire ?
=> POURQUUUUOOOIIII ? ? ?

> Ainsi, la fragmentation est désactivée par défaut sur les routeurs.

Ça existe uniquement "au cas où" c'est nécessaire.

> L'option MSS (Maximum Segment Size = taille maximale des données applicatives) de TCP, échangée dans les segments SYN, permet de limiter les risques de fragmentation des paquets IP véhiculant la connexion.



2. Pourquoi n'est-ce pas suffisant pour supprimer tout risque de fragmentation sur la

connexion?

Si sur le chemin se trouve un lien avec une MTU plus petite que le minimum des MTU extrémités au niveau des deux instances TCP.

> La mise en œuvre du Path MTU discovery (ou PMTUD) dans TCP est une façon de lever cette limitation reposant sur le postionnement du bit Don't Fragment des paquets IP utilisés.

3. Décrire l'utilisation du PMTUD dans une connexion TCP.

L'utilisation du bit *Don't Fragment* est utilisé (presque détourné car à la base c'est pas fait pour ça) afin de forcer les routeurs ayant une MTU trop basse à le signaler via ICMP : `Destination Unreachable : fragmentation needed with MTU=<<taille>>` suivi du début du message ayant posé problème afin de pouvoir l'identifier.
Ce message est envoyé à l'émetteur, et transmis à TCP (car IP s'en bat royalement les couilles, s'il faut c'est pas lui qui a envoyé le message mdrrr). Si connexion il y a, TCP va l'identifier grâce au morceau d'entête fourni par ICMP puis prendre les mesures nécessaire, à savoir recalculer la MSS puis découper lui-même en morceaux assez petits.

> Certains routeurs ou pare-feu sont parfois configurés pour ne pas acheminer de messages ICMP, jugés peu utiles et favorisant les attaques.

4. Qu'arrive-t-il à une connexion TCP utilisant le PMTUD qui traverse une telle passerelle ?

Elle plante (enfin elle ne va pas pouvoir détecter le problème ; c'est un trou noir. La connexion va timeout, RTO tout ça).

> Une autre technique, appelée MSS clamping repose sur la modification, à la volée, du champ MSS des segments TCP par une passerelle de niveau 3 reliant deux réseaux de MTU différentes.

5. En quoi cette solution est-elle plus efficace que la première mais moins générale que la deuxième ? Pourquoi est-elle (sous cette forme) peu satisfaisante ?

Elle change les réglages avant le début de la transmission et évite les erreurs avant qu'elles ne se produisent (plutôt que de détecter le problème a posteriori et le corrigé).

Nonobstant, elle nécessite que l'intégralité des routeurs supportent cette fonctionnalité pour fonctionner. En outre, si nous sommes amenés à changer de chemin, cela ne fonctionnera guerre.

6. Expliquer pourquoi ces diverses propositions ne peuvent que permettre de diminuer le risque de fragmentation et pourquoi ce phénomène ne disparaitra jamais

complètement à moins d'une remise en cause des caractéristiques fortes d'IP.

Nous ne possèderont jamais une vue globale sur le réseau. Ainsi, il existera toujours des cas qui ne fonctionneront pas.