Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Admin Réseau

TD n°4

QoS, TCP & Gestion de la congestion

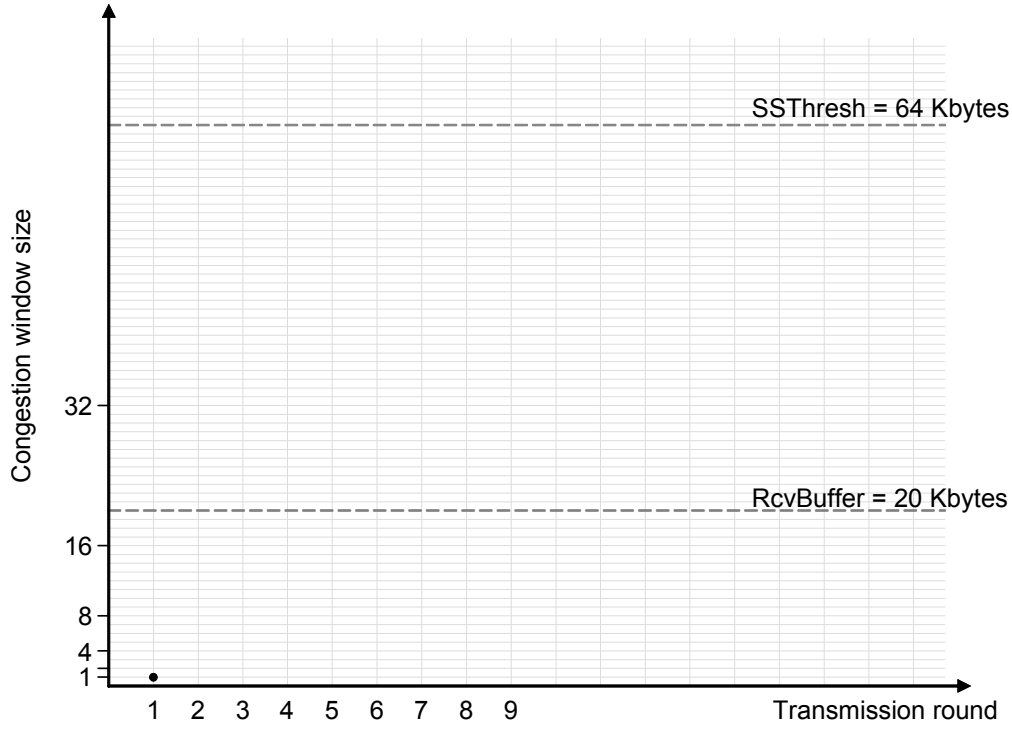
TCP & fenêtre de congestion

1 – Soient deux hôtes A et B connectés à un même réseau local avec un RTT, « *round-trip time* », négligeable. A envoie à B un gros volume de données en utilisant le protocole TCP :

- RcvBuffer = $20Ko$, le buffer de réception de B ;
- MSS = $1Ko$;
- le « ssthresh » = $64 * MSS$;

Il n'y a pas d'erreur de transmission, chaque hôte dispose d'un processeur rapide et les autres paramètres nécessaires sont standards.

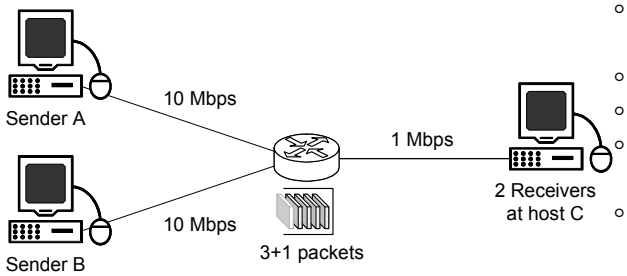
a. Tracer l'évolution de la fenêtre de congestion durant le « *slow-start* » pour un réseau de $100Mb/s$:



b. Comment évolue le tracé si le débit du réseau est réduit à $10Mb/s$? $1Mb/s$?

c. À quel étape l'émetteur entre en phase d'évitement de congestion, « *congestion avoidance* » ?

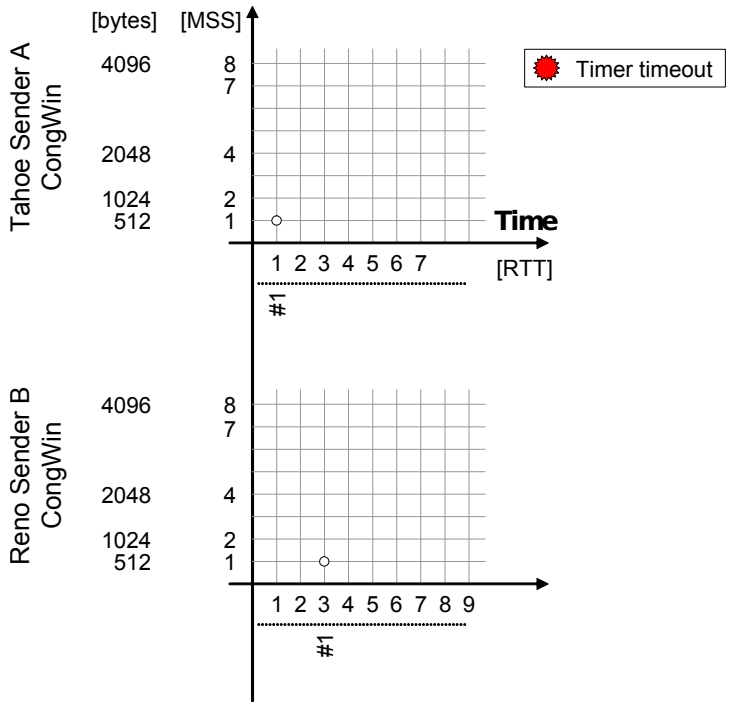
2 – Soit le réseau suivant :



- les hôtes A et B envoient par TCP $3,6Ko$ de données chacun, à l'hôte C ;
- la MTU est de $512octets$ pour tous les liens ;
- le $TimeoutInterval = 3 * RTT = 3 * 1sec$;
- le routeur dispose d'une capacité de 3 paquets en plus de celui actuellement transmis ;
- si le routeur doit détruire un paquet, il choisit le dernier paquet arrivé en provenance de l'hôte qui transmets le plus de paquets.

- le protocole TCP de l'hôte A exécute « TCP Tahoe » ;
- le protocole TCP de l'hôte b exécute « TCP Reno » ;
- l'hôte B commence sa transmission $2 * RTT$ après A.

a. Tracez l'évolution de la fenêtre de congestion sur les hôtes A et B.



On utilisera une grande fenêtre de réception, une transmission sans erreur sur tous les liens. Afin de simplifier le tracé, on considérera que tous les ACK arrivent exactement après un RTT et que la fenêtre de congestion est mise à jour à ce moment là.

Firewall & QoS

3 – Soit la configuration des routeurs :

Routeur	eth0	eth1	eth2
A	10.0.0.9/30	10.1.1.9/30	192.168.0.254/24
B	10.0.0.10/30	10.0.0.17/30	--
C	10.0.0.13/30	10.0.0.18/30	--
D	10.0.0.14/30	10.1.1.14/30	164.81.0.254/24
E	10.1.1.17/30	10.1.1.10/30	--
F	10.1.1.18/30	10.1.1.13/30	--

a. Retrouvez le schéma du réseau d'interconnexion de ces différents routeurs ;

b. On veut appliquer la politique de sécurité suivante :
   - ◇ on veut empêcher les machines du réseau `192.168.0.0/24` de communiquer vers l'extérieur de ce réseau ;
   - ◇ les machines du réseau `192.168.0.0/24` sont autorisées à accéder à un serveur Web d'adresse `164.81.16.41`.

   Indiquez le routeur à configurer et donnez la configuration utilisée avec `iptables` pour appliquer cette politique.

c. On veut empêcher l'accès SSH (port 22) depuis le réseau `164.81.0.0/24` sur le routeur D.
   Donnez la commande `iptables` à utiliser.

d. Soit la configuration suivante pour réaliser de la QoS :

```
# tc qdisc add dev $IF root handle 1: htb default 10
# tc class add dev $IF parent 1: classid 1:10 htb rate 20mbps
# tc class add dev $IF parent 1: classid 1:20 htb rate 10mbps
```

On veut limiter le trafic du protocole VNC à 10mbps. *Le protocole VNC est basé sur TCP (port 5900) et permet de visualiser l'écran d'un ordinateur à distance.* Sur quel routeur doit-on installer cette configuration de QoS, si l'accès par VNC se fait depuis une machine du réseau `192.168.0.0/24` vers une machine du réseau `164.81.0.0/24`
(c-à-d qu'une machine du réseau `164.81.0.0/24` envoi régulièrement le contenu de son écran à une machine du réseau `192.168.0.0/24`) ?
Indiquez quelles sont les commandes à utiliser pour mettre en œuvre cette QoS.