INFOB315 Télécommunications et Réseaux

Révisions

Année 2019-2020

Rappels

Dans le cours, on considère une version de TCP où :

— Au départ, `ssthresh` vaut ∞ et `CongWin` vaut 1.

— Quand `CongWin` $\leq$ `ssthresh`, l'émetteur est en *slow start* : la fenêtre croît de façon exponentielle (elle est augmentée de 1 à chaque acquittement reçu, et double donc à chaque fois qu'elle a pu être envoyée au complet).

— Quand `CongWin` $>$ `ssthresh`, l'émetteur est en *congestion avoidance* : la fenêtre croît de façon linéaire (elle est augmentée d'une fraction à chaque acquittement reçu, et augmente donc de 1 à chaque fois qu'elle a pu être envoyée au complet).

— Quand trois acquittements dupliqués sont reçus, on met à jour les valeurs de `ssthresh` et `CongWin` : tous deux valent à présent la moitié de l'ancienne valeur de `CongWin` (arrondie vers le bas), donc $\lfloor \frac{\texttt{CongWin}}{2} \rfloor$. On envoie le premier segment non acquitté et on repart alors en *congestion avoidance*.

— Quand un *timeout* survient, `ssthresh` est mis à $\lfloor \frac{\texttt{CongWin}}{2} \rfloor$ et `CongWin` est mis à 1. On envoie le premier segment non acquitté et on repart alors en *slow start*.

Question 1 (Janvier 2014)

Supposons que le client C demande au serveur S un objet en TCP. Le serveur S devra découper l'objet en 10 segments à envoyer au client C. Malheureusement, les 4e, 8e et 12e segments envoyés sont perdus. Voici les caractéristiques de la connexion :

— Débit de la ligne = R Mb/s,

— Segments de données = S bits (en-têtes comprises),

— Autres segments = A bits (en-têtes comprises),

— RTT = $\frac{3S}{R}$,

— RTO = $\frac{7S}{R}$.

Question 1.1 Dessinez le diagramme temporel du scénario, en indiquant clairement l'état de la `SWin`, ainsi que la valeur des variables `CongWin` et `ssthresh` de l'entité TCP sur le serveur S.

Question 1.2 Calculez le temps de téléchargement de l'objet par le client (établissement et fermeture de la connexion TCP compris) en considérant que la taille des ACKs est négligeable. Si vous avez besoin d'autres hypothèses, précisez-les.

Question 2 (Août 2019)

Alice souhaite transmettre un document à Cynthia. Malheureusement, elle ne peut la joindre directement, et doit passer par un intermédiaire, Bob, collègue de Cynthia.

Question 2.1 Mettez en place et décrivez un protocole qui assure les propriétés suivantes :

— Le document est transféré d'Alice à Bob de façon confidentielle.

— Il se peut que le document se perde lorsqu'Alice le transmet à Bob. Si le document est bien parvenu à Bob, Alice en est assurée (et elle est assurée que c'est bien Bob qui l'a reçu). Sinon, Alice renvoie le document à Bob.

— Cynthia peut vérifier que le document que Bob lui transmet en clair est effectivement le document envoyé par Alice.

Si vous faites des hypothèses supplémentaires, mentionnez-les (en justifiant) dans votre réponse. Utilisez les notations suivantes :

— m est le document,

— $H(.)$ est une fonction de hachage,

— $K^S_{X,Y}(.)$ est une clé de cryptographie symétrique partagée par X et Y,

— (K^+_X, K^-_X) est la paire de clés de l'intervenant X en cryptographie à clé publique.

Question 2.2 Formalisez le protocole sous la forme de trois machines à états finis (une par partie prenante).

Question 3 (Août 2019)

Voici la table de forwarding IPv6 d'un routeur R1.

Destination	Directement connecté	Interface/next hop
`2001:41d0:301:23::/64`	Oui	`eth_N`
`2001:41d0:301:12::/64`	Oui	`eth_S`
`FE80::/10`	Oui	`eth_W`
`2a01:428::/3`	Non	`2001:41d0:301:23::3`
`2606:6c00::/32`	Non	`2001:41d0:301:23::3`
`2001:c000::/19`	Non	`2001:41d0:301:12::1`
`2000:1f60::/32`	Non	`2001:41d0:301:12::1`
`2001:300:247:8000/49`	Non	`FE80::4`
`::/0`	Non	`FE80::4`

Question 3.1 Représentez l'architecture du réseau de façon graphique du mieux que vous le puissiez sur base de cette table de routage.

Question 3.2 L'entreprise va s'agrandir de trois nouveaux départements : le Département X, le Département Y et le Département Z. Au point de vue de son réseau, elle souhaite utiliser le préfixe `2001:41d0:301::/120` pour adresser ces trois nouveaux départements, dont les tailles sont estimées comme suit :

— Département X : 40 à 60 terminaux

— Département Y : 100 à 120 terminaux

— Département Z : 20 à 30 terminaux

Partagez le préfixe entre les trois départements, et complétez votre schéma précédent pour qu'il soit le plus réaliste possible en ce qui concerne l'ajout de ces trois départements. Vous pouvez ajouter tous les artefacts qui vous semblent utiles (routeurs, serveurs, sous-réseaux, ...).

Question 3.3 En cohérence avec les points précédents, adaptez la table de forwarding IPv6 de R1 pour que les nouveaux départements soient correctement incorporés au réseau de l'entreprise. Si vous avez ajouté de nouveaux routeurs au point précédent, donnez la table de forwarding IPv6 d'un de ces routeurs.

Corrigé examen 2020