

# Majeure Informatique - X01

Contrôle écrit : Réseaux, protocoles (INF 586)

Jeudi 25 mars 2004

Le contrôle dure 2h. Les questions sont indépendantes. Les documents sont autorisés.

## Question 1 (6 points)

Considérons un réseau linéaire  $S-R_1-R_2-D$  composé de trois liens reliant un nœud source  $S$  à un nœud destination  $D$  via deux routeurs intermédiaires  $R_1$  et  $R_2$ . Chaque routeur dispose d'une file d'attente de sortie de taille  $N$  paquets. Le délai de propagation sur chacun des liens est de  $d$  sec. Les liens ont chacun une capacité de  $C$  bps. Les paquets de données et les accusés de réception ont la même taille qui est égale à  $P$  bits. On considère que  $C$ ,  $d$  et  $P$  sont liés par la relation  $C \cdot d = nP$  où  $n$  est un entier. Le débit d'émission à la source est limité par la capacité du lien. La source utilise cependant un mécanisme de contrôle de flux par fenêtre. La valeur de la fenêtre est de  $W$ .

Le délai aller retour est défini comme étant la différence de temps entre l'instant où le premier bit d'un paquet de données est transmis sur le lien par  $S$  et l'instant où le dernier bit de l'accusé de réception correspondant est reçu par  $S$  (c'est à dire on ne tient pas compte du délai d'attente éventuel dans la file d'attente de sortie à la source). Si le paquet ou l'accusé de réception sont perdus, le délai aller-retour est considéré comme étant égal à zéro. On néglige le temps de traitement à la destination. Quant aux routeurs intermédiaires  $R_1$  et  $R_2$ , un paquet entrant est d'abord reçu complètement puis transmis immédiatement sur le lien de sortie s'il n'y a pas des paquets en attente dans la file d'attente de sortie (mode store and forward). Sinon, le paquet sera transmis après le service de tous les paquets dans la file. Un paquet reçu alors que la file est pleine est jeté.

1. Considérons d'abord que  $N = 2$  (un tampon mémoire est réservé pour le paquet en cours de réception ; et un autre contient le paquet en cours d'émission et sera libéré après l'émission complète du paquet). Calculer le délai aller retour en fonction des paramètres du réseau.
2. Même question pour  $N = 5$ . La source étant seule à émettre pourrait il y avoir des pertes de paquets dans les routeurs pour certaines valeurs de  $W$ ? Est ce que le délai de bout en bout change? Si oui comment évolue-t-il? sinon pourquoi?
3. On considère maintenant que les routeurs  $R_1$  et  $R_2$  sont liés à d'autres nœuds du réseau et qu'ils reçoivent un trafic exogène (en provenance d'autres sources) de façon à ce que les files d'attente de sortie ( $N=5$ ) soit tout le temps remplies à 60 % par ce trafic exogène. Quelle est la valeur du délai aller retour en fonction des paramètres du système?

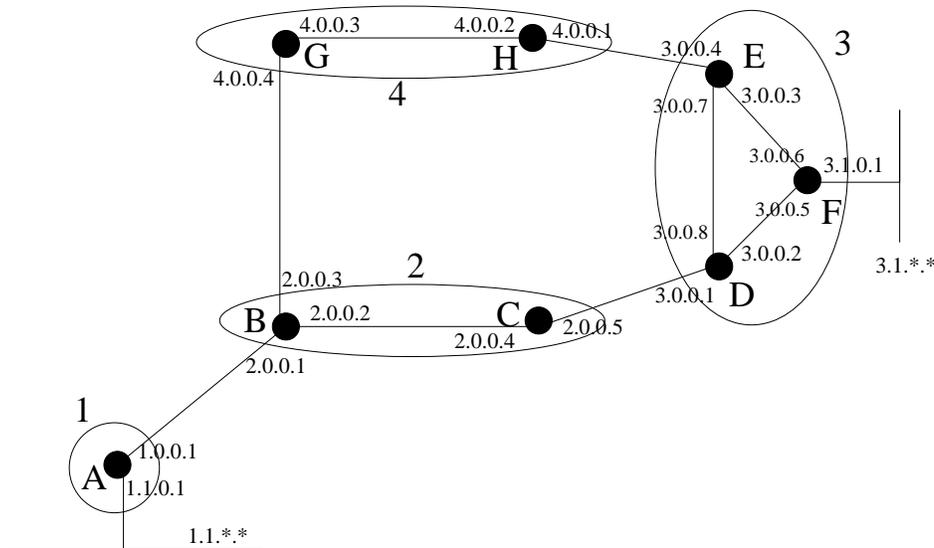
## Question 2 (4 points)

Ethernet est basé sur le mécanisme CSMA/CD pour la gestion de l'accès au canal partagé. Il s'agit donc de détecter les collisions et d'arrêter la transmission des paquets en cas de collision. On considère un segment Ethernet de longueur maximale  $L$  mètres. Soit  $C$  la capacité du lien Ethernet en bps. Soit  $v$  la vitesse de propagation du signal sur le lien en m/s.

1. Dire pourquoi les paquets Ethernet doivent avoir une taille minimum  $P_{min}$ .
2. Calculer cette taille minimum en fonction des paramètres ci-dessus.  
Application pour  $L = 10^3$ ,  $C = 10^7$  et  $v = 10^8$ .

3. On considère les réseaux Ethernet à 100 Mbps. Que devrait être alors  $P_{min}$  si on veut garder la même longueur maximale du segment Ethernet? Que faudrait il faire selon vous?

### Question 3 (5 points)



Des systèmes autonomes identifiés par les numéros 1, 2, 3, 4 sont reliés entre-eux par des liens inter-réseaux pour former le réseau de réseaux ci-dessus. Le système autonome 1 gère toutes les adresses 1.\*.\*. Le 2 gère 2.0.\*.\*, le 3 gère 3.\*.\* et le 4 gère 4.0.\*. Le système autonome 1 possède un seul routeur, A. Le 2 possède B et C, le 3 possède D, E et F, et le 4 possède G et H. Chaque routeur possède une adresse IP par interface. Les interfaces de B, par exemple, ont pour adresses 2.0.0.1, 2.0.0.2 et 2.0.0.3. De plus, A sert de passerelle ( gateway ) au sous-réseau 1.1.\*.\* (constitué d'un brin ethernet) auquel il est relié par 1.1.0.1. De même, F est la passerelle du sous-réseau 3.1.\*.\* auquel il est relié par 3.1.0.1.

On suppose que le protocole utilisé à l'intérieur d'un système autonome est de type état de liens ( link state ), comme OSPF. Entre les système autonomes, le protocole utilisé est de type vecteur chemin ( path vector ), comme BGP. (Un chemin sera constitué des numéros des systèmes autonomes à traverser pour atteindre un préfixe de réseau donné.)

Pour vérifier le fonctionnement du réseau, il est possible d'envoyer des paquets PING avec des temps de vie (TTL) quelconques. Le destinataire d'un PING répond par un paquet PONG. Si un routeur reçoit un PING avec TTL 0, il répond par un paquet d'erreur ICMP (l'adresse IP source du paquet ICMP est celle de l'interface par laquelle le routeur envoie le paquet). Un *traceroute* consiste à envoyer vers une destination des PINGS de TTL 0, 1, 2,... jusqu'à réception du PONG. La liste des adresses des routeurs intermédiaires qui répondent est alors établie.

1. Quelles seront les adresses listées pour un traceroute de 1.1.1.1 vers 3.1.3.3 ?
2. Pour chaque nœud sur la route de 1.1.1.1 à 3.1.3.3 (source et destination incluses), indiquer l'entrée dans la table de routage qui a permis de choisir le nœud suivant ( next hop ) sur la route, et indiquer les mécanismes qui ont conduit à insérer cette entrée dans la table (on précisera en particulier le protocole de routage qui a inséré l'entrée).
3. Quelles seraient les adresses listées pour un traceroute de 1.1.1.1 vers 3.1.3.3 après rupture du lien entre C et D (et après convergence des protocoles de routage) ?
4. On suppose que le lien CD se rétablit mais que C n'a pas encore fait passer l'information à B alors que D a informé E et F. Quelles seraient alors les adresses listées pour un traceroute de 1.1.1.1 vers 3.1.3.3 ?

5. Expliquer comment le problème du comptage à l'infini ( count to infinity ) sera évité si les liens  $CD$  puis  $EH$  cassent.

### Question 4 (3 points)

On considère une connexion TCP entre une source et une destination qui débute sur un réseau Ethernet, continue par exemple sur le réseau RENATER (réseau IP qui couvre la France), et se termine sur un réseau local distant. On considère la situation où le réseau local distant est un réseau sans fil. La *seule* caractéristique d'un réseau sans fil qui nous intéresse ici est la suivante: chaque paquet émis sur le réseau sans fil peut être perdu avec une probabilité  $p$ , et les pertes ont lieu *indépendamment* de l'état plus ou moins congestionné des réseaux Ethernet, RENATER, et sans fil.

Note: En pratique, ces pertes sont dues au fait que les réseaux sans fil utilisent des liaisons radio qui ne sont pas toujours fiables (à cause d'interférences électromagnétiques, de la pluie, de murs d'immeubles ou de bureaux). Il arrive donc que certains paquets arrivant du réseau RENATER soient perdus lors de la transmission radio.

a/ Quel est l'impact des pertes sur le lien sans fil sur les performances (en particulier le débit) de bout en bout de la connexion TCP?

b/ Si cet impact est positif, comment serait-il possible de l'augmenter? S'il est négatif, comment serait-il possible de l'éliminer? Pensez à évaluer le coût et la facilité d'implémentation des solutions que vous proposez (ces solutions peuvent nécessiter de modifier TCP).

### Question 5 (4 points)

Un mécanisme appelé "Packet Pair" (abréviation PP) a été proposé il y a quelques années. Comme son nom l'indique, PP envoie deux paquets l'un derrière l'autre et mesure l'intervalle entre ces paquets à la destination (ou l'intervalle entre les acquittements renvoyés vers la source, en supposant ces acquittements immédiats et non perturbés par leur passage dans le réseau).

Considérons d'abord une connexion dans un réseau où les routeurs sont de type FIFO. Que permet de mesurer la technique PP?

Considérons une connexion dans un réseau où les routeurs sont de type Fair Queueing. Montrez que PP permet de mesurer la capacité disponible pour cette connexion. Décrivez ensuite un mécanisme de contrôle de congestion basé sur PP. Discutez les avantages et inconvénients de ce mécanisme pour l'Internet.

## Question 1

1.  $N=2$  signifie que l'on dispose de tampons mémoire suffisants pour que la transmission stop and work fonctionne correctement. Le temps de transmission d'un paquet de données ou d'un accusé de réception est de  $P/C$ . Le délai aller retour (RTD) pour  $N=2$  est de  $6.P/C + 6.d = 6.P/C + 6.n.P/C = 6(n+1).P/C$ . Cette valeur est constante quelque soit la valeur de la fenêtre car le délai est calculé au niveau de la carte réseau de la source. Même si la fenêtre dépasse la taille du tuyau (qui est égale à  $6(n+1)$ ), il n'y aura ni augmentation du délai (les paquets seront mis en attente au niveau de la file d'attente de sortie de  $S$ ) ni perte des paquets dans le réseau (le lien  $S-R_1$  joue le rôle de régulateur de débit, et tous les liens ont la même capacité.)
2. Pour  $N = 5$ , les liens d'accès jouent toujours le rôle de lissage de trafic et le délai *dans le réseau* ne change pas:  $RTD = 6(n+1).P/C$ .  
Par ailleurs, il n'y a pas de perte de paquet quelque soit la valeur de la fenêtre.
3. Pour un trafic exogène qui remplit les files d'attente des  $R_i$  à 60 %, le délai augmente du temps de traitement de 3 paquets dans chaque sens. D'où  $RTD = 6(n+1).P/C + 6P/C = 6(n+2).P/C$   
Pas de débordement des files d'attente dans les routeurs car les liens d'accès lissent le trafic.

## Question 2

1. Considérons deux stations situées chacune d'une part et d'autre du segment Ethernet (séparées donc d'une distance maximale de  $L$ ). Si les paquets sont trop courts, il se peut que le début d'un paquet émis par une station ne s'est pas propagé jusqu'à l'autre bout du segment avant la fin de la transmission du paquet. Il est possible donc que deux stations (situées d'une part et d'autre du segment) commencent la transmission en même temps et au moment de la fin de la transmission du paquet à chaque station, le paquet en provenance de l'autre station n'est pas encore arrivé. Dans ce cas, les stations sur le réseau entre les deux stations pourraient détecter la collision (ce qui invalide la transmission des paquets), sans pour autant que les stations des deux bouts se rendent compte qu'il y a eu une collision. Il faudrait donc que le temps de transmission minimum d'un paquet dépasse le double du temps de propagation de bout en bout:
2.  $P_{min}/C \geq 2.L/v$ . Pour les valeurs indiquées, on choisit  $P_{min} = 200$  bits.
3. Si  $C = 10^8$ , alors  $P_{min} = 2000$  bits pour garder un segment de 1000 m. Or une taille minimum différente des paquets rend plus difficile l'interfonctionnement des deux versions d'Ethernet. On adopte alors le choix de réduire la taille maximum du segment qui devrait alors être de 100 m et on garde la même taille minimum de paquet.

## Question 3

1. On ne voit qu'une seule interface par routeur, celle de la route retour :  
1.1.0.1  
2.0.0.1  
2.0.0.4  
3.0.0.1  
3.0.0.5  
3.1.3.3

2.
  - 1.1.1.1 : routage par défaut vers la passerelle, entrée configurée manuellement ou par DHCP
  - A* : entrée pour 3.\*.\*.\* vers B d'après BGP
  - B* : entrée pour 3.\*.\*.\* vers C d'après OSPF
  - C* : entrée pour 3.\*.\*.\* vers D d'après BGP
  - D* : entrée pour 3.1.\*.\* vers F d'après OSPF
  - F* : entrée pour 3.1.\*.\* vers lien ethernet configuré manuellement
  - 3.1.3.3 : le paquet est arrivé le nœud a obtenu son adresse soit par configuration manuelle soit par DHCP

3.
  - 1.1.0.1
  - 2.0.0.1
  - 4.0.0.4
  - 4.0.0.2
  - 3.0.0.4
  - 3.0.0.6
  - 3.1.3.3

4. Les ICMP de *E* et *F* reviennent par *DC* :

- 1.1.0.1
- 2.0.0.1
- 4.0.0.4
- 4.0.0.2
- 3.0.0.7
- 3.0.0.5
- 3.1.3.3

5. Quand *CD* casse, les routeurs de 2 utilisent 2 – 4 – 3 pour atteindre 3.\*.\*.\*. Quand *EH* casse, les routeurs de 4 n'essayeront pas de passer par 2 puisque leur chemin contient 4. Ils annoncent donc une distance infinie et les routeurs de 2 feront alors de même.

## Question 4

a/ Les pertes dues aux erreurs de transmission seront interprétées comme des signaux de congestion et vont provoquer une réduction du débit de la source TCP.

b/ L'impact est donc négatif et il est à éliminer.

Trois solutions sont citées:

1. protéger le lien par des mécanismes de FEC au niveau lien qui réduisent le débit disponible à l'utilisateur mais facilitent le support transparent du protocole
2. scinder la connexion TCP en deux et modifier le protocole pour arrêter les contrôle de congestion sur la partie radio. Cette solution ne modifie pas la couche liaison, mais nécessite des modifications de TCP.
3. inférer à partir du profil des pertes et des délais (corrélation entre les deux) s'il s'agit d'une perte due à la corruption ou à la congestion et adopter le comportement approprié au niveau TCP. Cette solution permet de garder l'esprit de bout en bout du protocole mais est difficile à réaliser.

## Question 5

Vu que l'espacement des paquets à la sortie du goulot d'étranglement est inversement proportionnel à la bande passante du lien de sortie de routeur, la technique PP permet de mesurer la bande passante du lien de sortie du goulot d'étranglement.

Si le routeur est FQ, les paquets des différentes connexions seront servis à tour de rôle et l'espacement sera alors inversement proportionnel à la bande passante disponible pour la connexion considérée. La source pourra alors mesurer la bande passante disponible pour elle et adapter son débit judicieusement. La technique FQ assure l'équité entre les connexions et donc la protection des connexions les unes des autres. Il suffit donc que la source s'adapte à bande passante qui lui est disponible. En FIFO, les deux paquets reçus seront servis l'un à la suite de l'autre et dans ce cas PP permet de mesurer la capacité (temps de service d'un paquet) du lien de sortie du routeur goulot d'étranglement. Donc ne permet pas facilement de concevoir un mécanisme de contrôle de congestion.