Réseaux 6e édition

Andrew Tanenbaum, Nick Feamster, David Wetherall

Corrigés des exercices

Chapitre 5 : La sous-couche Réseau

ISBN : 978-2-3260-0239-5

1. Oui. Les signaux d'interruption doivent passer avant les données et donc être transmis hors séquence. C'est le cas lorsque l'utilisateur frappe la touche d'abandon pour quitter (kill). Le paquet que produit cette action doit être envoyé en priorité en passant avant les données en attente d'envoi, c'est-à-dire saisies mais pas encore lues.

2. Quatre sauts impliquent cinq routeurs. L'implémentation en circuit virtuel requiert de réunir 5 x 8 = 40 octets de mémoire pour 1000 s. L'implémentation en datagramme demande de transférer 12 x 4 x 200 = 9600 octets d'en-tête en plus des besoins du circuit virtuel. La question revient donc à comparer le coût de 40 000 octets-seconde de mémoire à celui de 9 600 octets-sauts de capacité de circuit. Si la mémoire est dépréciée après 2 x 52 x 40 x 3600 = 1,5 x 10^7 secondes, un octet-seconde revient à 6,7 x 10^{-8} cents, et 40 000 coûtent un peu plus de 2 millicents. Si un octet-saut vaut 10^{-6} cents, une quantité de 9 600 vaut 9,6 millicents. Les circuits virtuels sont donc plus économiques pour ce jeu de paramètres.

3. Au départ : *B*: 1 via *A*, *C*: 2 via *B*, *D*: 3 via *C*, *E*: 4 via *D*. Après 1 échange : *B*:, *C*: 2 via *B*, *D*: 3 via *C*, *E*: 4 via *D*. *B* constate alors que *A* est injoignable parce que *B* n'en reçoit rien directement ; le chemin de *C* vers *A* passe par *B*. Après 2 échanges : *B*: , *C*: , *D*: 3 via *C*, *E*: 4 via *D*. *C* constate alors que *A* est injoignable parce que *B* n'a pas publié de chemin vers *A*, et le chemin de *D* vers *A* passe par *C*. Après deux autres échanges, *D* et *E* sont également informés que *A* n'est plus joignable.

4. Le calcul du chemin le moins cher vers chaque destination depuis *D* donne (8, 5, 3, 0, 6, 4). Les lignes sortantes sont (*C*, *F*, *C*, –, *C*, *F*).

5. Il va suivre toutes les routes suivantes : *ABCD*, *ABCF*, *ABEF*, *ABEG*, *AGHD*, *AGHF*, *AGEB* et *AGEF*. Le nombre de sauts est de 24.

6. Cherchez une route utilisant le chemin le plus court. Effacez tous les arcs utilisés sur la route retenue et renouvelez l'algorithme de plus court chemin. Ce deuxième chemin est susceptible d'être utilisé en cas de défaillance d'un élément (ligne, routeur) du premier chemin. Pour augmenter l'efficacité, il est possible de recommencer l'expérience afin de découvrir un troisième chemin.

7. Aller par *B* donne (11, 6, 14, 18, 12, 8).

   Aller par *D* donne (19, 15, 9, 3, 9, 10).

   Aller par *E* donne (12, 11, 8, 14, 5, 9).

   En prenant le minimum pour chaque destination, à l'exception de C, on obtient (11, 6, 0, 3, 5, 8). Les lignes de sorties sont (*B*, *B*, –, *D*, *E*, *B*).

8. Les algorithmes de routage gèrent des structures descriptives dans les routeurs et les maintiennent à jour pour disposer d'une vue du réseau réel. Ces structures sont exploitées par la transmission et la commutation pour déteminer où envoyer les paquets, tant dans les réseaux sans connexion que ceux avec connexion. La procédure est assez simple dans le cas de la commutation, puisqu'elle peut se limiter à la recherche d'un label de paquet dans une table. Dans le cas de la transmission, il y a plus de calculs, par exemple lorsqu'il faut trouver le plus long préfixe correspondant, mais ces définitions ne sont pas universelles.

9. Cela vaut dans tous les cas. Si un paquet est arrivé sur une liaison donnée, il doit être acquitté, ce qui provoque l'envoi d'un paquet sur cette même liaison. Au contraire, si un paquet n'est pas arrivé sur une liaison donnée, on doit le réexpédier (vers un autre routeur) sur cette liaison. Les cas 00 (pas arrivé, pas renvoyé) et 11 (arrivé et réexpédié) sont logiquement incorrects et n'existent pas.

10. Le minimum apparaît avec 15 grappes, chacune avec 16 régions, et chaque région dispose de 20 routeurs. Autre forme : 20 grappes, 16 régions, 15 routeurs. Dans chaque cas, la taille de la table de routage est égale à 15 + 16 + 20 = 51.

11. L'agent de domiciliation dupe le routeur qui se fait passer pour le mobile, en répondant aux requêtes ARP qui lui sont destinées. Lorsque le routeur détecte l'adresse IP du mobile dans un paquet entrant, il émet une requête ARP à destination de la machine associée à cette adresse, en lui demandant son adresse MAC 802.3. Si le mobile n'est pas présent (s'il s'est déclaré absent auprès de l'agent de domiciliation), c'est l'agent qui répond à la requête ARP à sa place, en lui transmettant son adresse MAC 802.3. Ainsi le routeur associe l'adresse MAC du mobile à celle de l'agent sans le savoir.

12. a) La réalisation de l'algorithme RPF nécessite 5 sauts. Les destinataires des paquets sont respectivement *AC*, *DFIJ*, *DEGHIJKN*, *GHKN* et *LMO*. Au total, 28 paquets ont été générés.

    b) Quant à l'arbre collecteur, il nécessite 4 sauts et la génération de 14 paquets.

13. Le nœud *F* a deux descendants, *A* et *D*. Il en acquiert à présent un troisième, *G* qui n'est pas cerclé car le paquet empruntant *IFG* ne fait pas partie de l'arbre collecteur. Le nœud *G* acquiert lui aussi un second descendant en plus de *D*, il s'agit de *F*. Lui non plus n'est pas cerclé, il ne fait pas partie de l'arbre collecteur.

14. Si le lien entre hôte émetteur et routeur offre un meilleur débit que celui entre routeur et récepteur, les tampons mémoire du routeur vont déborder, ce qui déclenche une congestion réseau. Si les deux liens ont le même débit mais que l'émetteur et le routeur supportent un débit supérieur à celui supporté par le récepteur, ce dernier ne réussira pas à tenir le rythme d'arrivée des paquets.

15. Ce protocole est épouvantable. Considérons des slots de T secondes. Au slot 1, le routeur source envoie son premier paquet. Au début du slot 2, le deuxième routeur a reçu le paquet mais ne l'a pas encore acquitté. Au début du slot 3, le troisième routeur a reçu le paquet mais il ne l'a pas encore acquitté, et ainsi de suite ; tous les routeurs derrière lui sont également suspendus. Le premier acquittement peut être transmis lorsque le dernier routeur a remis le paquet à l'hôte destinataire. Ce n'est qu'à partir de ce moment que les acquittements peuvent être transmis en retour. Cela prend un délai de deux traversées complètes du réseau, soit $2(n-1)\,T$ secondes, avant que le routeur source n'envoie son deuxième paquet. Le débit utile avec ce protocole est donc de 1 paquet toutes les $2(n-1)\,T$ secondes.

16. Chaque paquet émis par l'hôte source met 1, 2 ou 3 sauts. La probabilité qu'il mette 1 saut est de p. La probabilité qu'il mette 2 sauts est de $p(1-p)$. La probabilité qu'il mette 3 sauts est de $(1-p)^2$. Le nombre moyen de sauts qu'un paquet met pour atteindre sa destination est alors la somme de ces trois probabilités, soit $p^2 - 3p + 3$. Notez que pour $p = 0$, la moyenne est de 3 sauts, que pour $p = 1$, elle est de 1 saut. Avec $0 < p < 1$, des transmissions multiples peuvent apparaître. On obtient le nombre moyen de transmissions en prenant en compte le fait que la probabilité d'une transmission réussie est de $(1-p)^2$, probabilité que nous appelons α. Le nombre moyen de transmissions est alors égal à :

    $\alpha + 2\alpha\,(1-\alpha) + 3\alpha\,(1-\alpha)^2 + \ldots = 1/\alpha = 1/(1-p)^2$

    Enfin, le nombre de sauts nécessaires est de $(p^2 - 3p + 3) / (1-p)^2$.

17. Tout d'abord, la méthode ECN qui consiste à envoyer explicitement une notification de congestion à la source tandis que la méthode RED notifie simplement qu'un paquet a été mis à la poubelle. Ensuite, la méthode du bit d'avertissement met un paquet à la poubelle uniquement lorsqu'il n'y a plus de buffer disponible, alors qu'avec RED les paquets sont mis à la poubelle avant que tous les buffers ne soient épuisés.

18. Les transferts de fichiers volumineux peuvent entraîner l'envoi de grandes fenêtres de congestion pendant le temps d'un aller-retour. Lorsque l'on envoie en une fois un grand nombre de paquets, les paquets des autres applications restent en attente, ce qui augmente la latence. Les applications en temps réel le supportent difficilement tout comme les envois de petits fichiers car les temps d'aller-retour augmentent, ce qui impacte fortement la durée des petits transferts.

19. Utilisez un seau à jeton avec un débit de sortie de 20 Mbit/s.

20. 10 millions d'octets.

21. 140 secondes.

22.

Paquet	Heure de fin	Ordre de sortie
A	**08.00**	**1**
B	**08.00**	**2**
C	**15.00**	**4**
D	**12.50**	**3**
E	**23.00**	**6**
F	**16.00**	**5**
G	**33.00**	**8**
H	**24.00**	**7**

23. Désignons Δt la longueur de l'intervalle de rafale maximal. Dans le pire des cas, le seau est plein en début d'intervalle (1 Mo) et $10\Delta t$ Mo de plus arrivent pendant ce laps de temps. Pendant la rafale de transmission, la sortie contient $50\Delta t$ Mo. Nous pouvons poser l'équation $1 + 10\Delta t = 50\Delta t$ et la résoudre pour aboutir à un Δt de 25 ms.

24. Les réservations depuis les hôtes 3 et 4 vers l'hôte 1 se partagent 2 Mo/sec entre le routeur *H* et l'hôte 1. Les réservations depuis les hôtes 3 et 5 vers l'hôte 2 se partagent 1 Mo/sec entre le routeur *H* et l'hôte 2. Les bandes passantes en Mo/s sont :

    A : 2 vers E ; *B* : 0 ; *C* : 1 vers E ; *E* : 3 vers H ;

    H : 3 vers J, 2 vers K et 1 vers L ;

    J : 3 vers hôte 3 ; *K* : 2 vers hôte 4 et *L* : 1 vers hôte 5.

25. Dans notre cas, $\mu = 2$ millions, $\lambda = 1{,}5$ million et $\rho = \lambda/\mu$ soit 0,75. Selon la théorie des files d'attente, il apparaît que chaque paquet passe en moyenne un temps 4 fois plus élevé lorsque le système est bien chargé (file remplie) que lorsque le système est oisif (file vide). Le temps moyen de transit dans un système oisif est de 500 ns, il est dans notre cas de 2 μs. Avec 10 routeurs identiquement chargés sur un chemin, le temps de service total est donc de 20 μs.

26. Il n'y a pas de garantie. Si de trop nombreux paquets sont transmis, le canal qui les achemine verra ses performances se dégrader.

27. La charge utile IP à envoyer pèse 920 octets avec un en-tête IPv4 de 20 octets. Le premier lien pouvant traiter des paquets pesant jusqu'à 1010 octets, il n'y aura aucune fragmentation. Le deuxième lien est limité à 504 octets par paquet, ce qui obligera à fragmenter. Il pourra y avoir jusqu'à 484 octets de données, mais tous les fragments sauf le dernier doivent contenir un multiple de 8 octets. Le premier fragment contiendra donc 480 octets de données et le second 440. Le troisième lien accepte jusqu'à 500 octets par fragment et convient donc aux deux fragments.

    Le datagramme IP initial est fragmenté en deux datagrammes IP dans R1. Aucune autre fragmentation n'intervient ensuite.

    Ligne *A-R1* :

Longueur = 940, *ID* = x, *DF* = 0, *MF* = 0, *offset* = 0

Ligne *R1-R2* :

(1) *Longueur* = 500, *ID* = x, *DF* = 0, *MF* = 1, *offset* = 0

(2) *Longueur* = 460, *ID* = x, *DF* = 0, *MF* = 1, *offset* = 60

Ligne *R2-B* :

(1) *Longueur* = 500, *ID* = x, *DF* = 0, *MF* = 1, *offset* = 0

(2) *Longueur* = 460, *ID* = x, *DF* = 0, *MF* = 1, *offset* = 60

28. Si le débit sur la ligne est *b*, le nombre de paquets par seconde que peut émettre le routeur est de *b*/8192. Transmettre 65 536 paquets prend $2^{29}/b$ secondes. En égalant cette expression avec la durée de vie maximale du paquet, on obtient $2^{29}/b = 10$. Ce qui donne $b = 53\,687\,091$ bit/s.

29. Comme l'information est nécessaire pour router chaque fragment, l'option doit apparaître dans tous les fragments.

30. Avec un préfixe de 2 bits, il resterait 18 bits pour coder le réseau. En conséquence, le nombre de réseaux identifiables serait de 2^{18}, soit 262 144. Toutefois comme les codes « tout à 0 » et « tout à 1 » sont réservés, le nombre total de réseaux serait de 262 142.

31. L'adresse IP est : 194.47.21.130.

32. Avant tout, les machines hôtes doivent être bi-modes avec une adresse IPv4 et une adresse IPv6, quitte à ne communiquer qu'en IPv4. Une autre solution consiste à faire passer les paquets IPv6 par un tunnel IPv4 : un routeur intermédiaire emballe un paquet IPv6 dans un paquet IPv4 puis le transmet par tunnel au réseau destinataire équipé en IPv6.

33. Le masque faisant 20 bits de long, la part pour coder le réseau est de 20 bits. Il reste 12 bits pour coder l'hôte, ce qui correspond à 4 096 adresses d'hôtes.

34. Toute carte ou tout adaptateur Ethernet dispose d'une adresse MAC unique qui lui est affectée lors de sa fabrication. Cette adresse n'a aucune relation avec un quelconque réseau, qu'il soit réseau IP ou autre. Elle facilite le routage et permet l'acheminement des trames sur un réseau Ethernet. Quant à l'adresse IP, elle est attribuée de façon fixe (statique) ou dynamique par un fournisseur d'accès à l'Internet. Elle permet d'identifier aisément une machine (ordinateur) sur un réseau.

35. Tout d'abord, signalons que toute adresse ne peut être qu'une puissance entière de 2. L'adresse de début, l'adresse de fin et le masque sont donnés ci-après :

    A : 198.16.0.0 – 198.16.15.255 écrit sous la forme 198.16.0.0/20

    B : 198.16.16.0 – 198.23.15.255 écrit sous la forme 198.16.16.0/21

    C : 198.16.32.0 – 198.47.15.255 écrit sous la forme 198.16.32.0/20

    D : 198.16.64.0 – 198.95.15.255 écrit sous la forme 198.16.64.0/19

36. Elles peuvent être agrégées en 57.6.96/19.

37. Il suffit d'ajouter une nouvelle entrée dans la table : 29.18.0.0/22 pour le nouveau bloc. Si un paquet entrant établit une correspondance avec les deux entrées 29.18.0.0/17 et 29.18.0.0/22, c'est le bloc de masque le plus long qui l'emporte.

38. La plage d'adresses agrégée du routeur A est 37.62.0.0/16 et celle du routeur B est 37.60.0.0/15. Si la table de routage du routeur C ne contient que ces deux entrées, les paquets dont l'adresse fait partie de la plage 37.62.64.0/18 sont incorrectement transmis au routeur A, alors qu'ils devaient l'être au routeur B. Le souci est l'agrégation qui produit un préfixe plus court. Une parade consiste à n'agréger que des plages contigües. Voir aussi : *https://tools.ietf.org/html/rfc4632*.

39. Avec NAT, il est crucial que tous les paquets associés à une même connexion externe entrent dans l'entreprise et en sortent par le même routeur. Si chaque routeur a sa propre adresse IP et que tout le trafic destiné à une même connexion soit acheminé par un même routeur, le mappage est réalisé plus efficacement avec NAT.

40. Le boîtier NAT lit le numéro de port dans les paquets entrants pour connaître l'adresse interne et le numéro de port. Il constate que l'entrée de table correspondante est vide (parce que le serveur n'a encore rien envoyé) et jette le paquet. Pour remédier à la situation manuellement, il faut configurer le NAT situé entre le serveur et Internet pour retransmettre au serveur les paquets entrants ayant le numéro de port concerné. On peut aussi positionner le serveur en sorte de ne plus être séparé d'Internet par le boîtier NAT. Vous et votre ami pouvez alors vous connecter directement au serveur.

41. Cela est possible parce que les machines ont des adresses IP différentes. Avec un boîtier NAT, les machines ont la même adresse IP extérieure, et le boîtier se base sur sa table de correspondance de port pour que les machines puissent utiliser le même numéro de port.

42. ARP ne fournit pas de service à la couche réseau, c'est un service de la couche réseau. Il permet à la couche réseau d'offrir un service à la couche transport. La traduction d'une adresse IP n'intervient pas à la couche liaison. Les protocoles de la couche liaison sont, comme les protocoles 1 à 6 du chapitre 3, HDLC, PPP, etc. Ils ont pour objectif de transmettre des bits sous forme d'une trame structurée entre les deux extrémités d'une liaison de données.

43. Le réseau sans fil est créé par le modem fourni par le FAI. Il sert aussi de passerelle par défaut pour le réseau privé avec par convention l'adresse la plus basse du réseau. Avec l'adresse IP fournie 192.168.0.103, cette adresse la plus basse est 192.168.0.1.

44. Dans le cas général, le problème n'est pas trivial. Les fragments peuvent arriver dans le désordre, certains peuvent être détruits ou perdus. Lors d'une retransmission, le datagramme peut être fragmenté en morceaux de tailles différentes. De plus, la taille totale du datagramme n'est pas connue tant que le dernier fragment n'est pas arrivé. La façon de faire la plus efficace est sans doute de mettre les fragments dans un buffer afin de reconstituer le datagramme une fois que le dernier fragment est arrivé et que sa longueur est connue. Il suffit donc de disposer d'un buffer de taille suffisante, d'y insérer les fragments arrivant, et d'y associer un tableau permettant de suivre l'évolution du remplissage du buffer et de savoir quels octets y sont présents. Quand la table est remplie, tous les fragments du datagramme sont présents.

45. Lorsque le récepteur reçoit un fragment, il le place en file d'attente jusqu'à ce qu'il reçoive les autres fragments. S'il ne les reçoit pas, à l'expiration du temporisateur, les divers fragments en mémoire tampon sont éliminés.

46. Une erreur dans l'en-tête est beaucoup plus grave qu'une erreur dans les données. Par exemple, une mauvaise adresse peut entraîner la remise d'un paquet à un mauvais destinataire. Nombre d'hôtes ne vérifient pas si les paquets qu'ils reçoivent leur sont réellement destinés. Ils considèrent que le réseau ne leur remet jamais de paquets destinés à un autre hôte. Les données non plus ne sont pas toujours vérifiées pour des raisons de coût. D'autant plus que les applications vérifient le plus souvent l'intégrité des données. Cela permet d'éviter les redondances d'actions et d'améliorer ainsi les performances.

47. Oui. Le fait que le LAN de Minneapolis soit sans fil est sans importance. L'agent de domiciliation de Boston établit un tunnel avec l'agent extérieur du réseau LAN sans fil de Minneapolis et renvoie le trafic de Boston à Minneapolis sans problème. La seule contrainte à respecter est celle, fonctionnelle, imposée aux utilisateurs par le LAN de Minneapolis (raccordement, protocole d'accès radio, etc.).

48. Avec 16 octets, on dénombre 2^{128} ou $3{,}4 \times 10^{38}$ adresses. Si on attribue ces adresses à la vitesse de 10^{18} adresses par seconde, cela prendra 10^{13} années pour les affecter toutes. Cela correspond à 1 000 fois l'âge de l'Univers. Bien sûr, toutes les adresses ne sont pas toutes possibles, certaines sont réservées, d'autres sont inaccessibles. Elles ne sont pas non plus allouées de façon linéaire. Toutefois, même si on ne considère qu'un espace réduit à 1/1 000 (soit 0,1 % de l'espace), le nombre d'adresses disponibles est toujours immensément important.

49. Avec des adresses IP permanentes, le routage est beaucoup plus difficile à rendre efficace. La taille des tables de routage reste actuellement gérable grâce à une utilisation hiérarchique de l'espace d'adresses. Si n'importe quelle adresse était utilisable de n'importe où sur Terre, cela ne serait plus possible.

50. Le champ *Protocole* précise à l'hôte quel protocole doit gérer le datagramme arrivant. Les routeurs n'ont pas besoin de cette information, elle ne les concerne pas. Il n'est donc pas nécessaire que ce champ soit présent dans l'en-tête principal du datagramme. Le champ *Extension d'en-tête* est notamment utilisé à cet effet.

51. Conceptuellement, il n'y a aucun changement. Techniquement les adresses IPv6 sont plus longues, il est donc nécessaire de disposer de champs plus longs.

52. Les questions 52 à 55 sont des travaux pratiques à faire éventuellement évaluer par un enseignant ou un expert.