heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Téléinformatique

Exercices & corrigés

Jeremy Berthet, Reynald Borer, Etienne Carrupt,
Gilles Doge, Murielle Savary

–

IL2007

13 juillet 2006

1 Notions de bases

1.1 Qu'est-ce qu'un réseau LAN, MAN, WAN ?

- LAN : un réseau d'envergure limitée à un bâtiment ou un groupe de bâtiment proches les un des autres. Couvre des distances de quelques centaines de mètres.
- MAN : un réseau liant plusieurs point d'une même ville entre eux. Il permettrais d'interconnecter les succursales d'une entreprise sur des distances de quelque kilomètres.
- WAN : un réseau d'envergure nationale ou internationale reliant plusieurs villes ou plusieurs pays entre eux. L'ordre de grandeur est de plusieurs centaines de kilomètres à plusieurs millier des kilomètres.

1.2 Pourquoi les réseaux WAN ont-ils pour la plupart une topologie en anneau ou maillée ?

Pour offrir une meilleure tolérance aux pannes. Lors de la panne d'un lien ou d'un nœud intermédiaire, un autre chemin peut être trouvé pour acheminer les données.

1.3 Quels avantages un réseau à commutation de circuits présente-t-il par rapport à un réseau à commutation par paquets ?

- temps de transit très cours ;
- qualité de transmission constante durant toute la communication.

1.4 Supposez que vous soyez en train de développer une norme pour un nouveau type de réseau. Vous devez choisir entre l'emploi de circuits virtuels ou le recours à un acheminement de datagrammes. Quels sont les arguments pour et contre l'utilisation de circuits virtuels.

Pour

- connexion fiable ;
- pas besoin de trouver un chemin à chaque fois ;
- le routage est plus rapide.

Contre

- maintien des informations sur l'état des connexions ;
- utilisation plus complexe et installation plus cher ;
- perte de fiabilité.

1.5 Imaginez le transfert d'une série de paquets entre un serveur émetteur et un hôte recepteur le long d'un chemin donné. Citez les différents types de retards composant le temps de transfert d'un paquet.

- Temps de traitement : temps requis au medium pour l'examen de l'entête du paquet et la détermination de la sortie à utiliser.

– Temps d'attente : temps passé par le paquet dans la file d'attente du medium.
– Temps de transmission : temps nécessaire au medium pour envoyer le paquet.
– Temps de propagation : temps nécessaire au paquet pour parcourir physiquement la liaison.

1.6 Supposez qu'un lien point-à-point à 100 Mb/s soit mis en place entre la terre et une colonie lunaire. La distance de la lune à la terre est d'environ 390'000 km et les données voyagent sur le lien à la vitesse de la lumière, 300'000 km/s.
a) Calculer le RTT minimum pour le lien.
b) En utilisant le RTT comme délai, calculez le produit délai*largeur de bande du lien.
c) Quelle est la signification du produit délai*largeur de bande calculé en b) ?

a) RTT (Round-Trip Time) : temps que met un paquet pour effectuer un aller-retour sur une ligne donnée. Le RTT est égale au double du temps de propagation (aller-retour).

$$\text{RTT} = 2 \cdot \frac{390'000 \text{ km}}{300'000 \text{ km/s}} = 2.6 \text{ s}$$

b) Le produit délai * largeur de bande vaut

$$\text{produit} = \text{RTT} \cdot \text{largeur de bande} = 2.6 \text{ s} \cdot 100 \text{ Mb/s} = 260 \text{ Mb}$$

c) Ce produit donne le nombre de bits se trouvant sur le lien (volume de données maximum qu'il est possible d'avoir au sein d'un medium à un moment donné). Il veut aussi dire que 260 Mb seront envoyés avant que le premier bit d'acquittement ne soit reçu.

1.7 Pour chacune des applications suivantes, expliquez si elles sont susceptibles d'être sensible au délai ou à la largeur de bande.
a) Voix sur IP (voice over IP)
b) Netmeeting (vidéo)
c) Chargement de fichiers MP3 et DivX

a) **Voix sur IP :** Sensible au délai. Pour assurer la transmission en direct de la parole, on ne peut pas attendre un paquet qui serait en retard. Il y a interruption de l'interactivité.

b) **Vidéo :** Sensible au délai pour la même raison que précédemment. Également sensible à la largeur de bande, si la bande passante est trop petite, il n'y a aucune chance que le débit soit suffisant pour permettre l'affichage correcte de la vidéo (saccade).

c) **Chargement de fichiers :** Le téléchargement de fichiers n'est pas sensibles à ces phénomènes, car on peut attendre que les paquets arrivent à leur rythme (peu importe l'ordre) et recomposer le ficher une fois tous les paquets reçus.

1.8 Quelle est la « largeur » (en secondes) d'un bit sur un lien 1 Gb/s ?

$$\frac{1 \text{ b}}{1 \text{ Gb/s}} = \frac{1 \text{ b}}{1 \cdot 10^9 \text{ b/s}} = 10^{-9} \text{ s} = 1 \text{ ns}$$

1.9 Vous cherchez à envoyer un long fichier de F bits d'un hôte A à un hôte B. Deux liaisons et un commutateur relient A et B. Supposez que les délais d'attente sont négligeables. L'hôte A segmente le fichier en segments de S bits et ajoute à chacun 40 bits d'entête, formant des paquets d'une longueur de L = S + 40 bits. Chaque liaison se caractérise par un débit de R bits/s. Trouvez la valeur de S minimisant le délai encouru par le fichier complet sur son parcours entre A et B, tout en négligeant le délai de propagation.

Schématiquement A → C → B

- A et B sont les deux extrêmités du réseau ;
- C est le commutateur, considérons le comme un routeur ;
- les flèches représentent les liaisons.

On néglige les délais de propagation. Il faut donc prendre en compte les délais de traitement et de transmission. Le délai de traitement est constant et n'est pas indiqué dans la donnée, on le considère donc comme négligeable.

- nombre de paquets à transmettre : $N = \frac{F}{S}$;
- temps de transmission : $T_{transm} = \frac{L}{R}$;
- temps de transfert du fichier :

$$\begin{aligned} T_{transf} &= (N+1) \cdot T_{transm} = (\frac{F}{S} + 1) \cdot \frac{S+40}{R} = \frac{F}{S} \cdot \frac{S+40}{R} + \frac{S+40}{R} \\ &= \frac{F \cdot S + 40 \cdot F}{R \cdot S} + \frac{S^2 + 40}{R \cdot S} = \frac{S^2 + (40+F) \cdot S + 40 \cdot F}{R \cdot S} \end{aligned}$$

Il faut donc chercher à quel moment la dérivée de T_{transf} est nulle, représentant un minimum ou un maximum de la courbe.

$$\begin{aligned} T'_{transf} &= \frac{S^2 - 2 \cdot (F+20)}{R \cdot S^2} \\ T'_{transf} &= 0 \Rightarrow S = \sqrt{2 \cdot (F+20)} \end{aligned}$$

1.10 Soit deux serveurs A et B connectés l'un à l'autre au moyen d'une seule liaison à R bits/s. Supposez que les deux serveurs soient séparés par une distance de m mètres et supposez que la vitesse de propagation le long de la liaison est de v m/s. Le serveur A envoie un paquet de L bits à l'hôte B.
a) Exprimez le temps de propagation d_{prop} en fonction de m et v.
b) Déterminez le temps de transmission du paquet d_{trans} en fonction de L et R.
c) Supposez que le serveur A commence à transmettre le paquet au temps $t = 0$. Où se trouve le dernier bit du paquet à l'instant $t = d_{trans}$?
d) Soit d_{prop} supérieur à d_{trans}. À l'instant $t = d_{trans}$ où est le premier bit du paquet ?
e) Soit d_{prop} inférieur à d_{trans}. À l'instant $t = d_{trans}$ où est le premier bit du paquet ?

a) Délai de propagation : $d_{prop} = \frac{m}{v}$.

b) Délai de transmission : $d_{trans} = \frac{L}{R}$.

c) Le dernier bit vient d'être transmis, il se trouve dans la liaison entre les deux serveurs (position $= m - v \cdot d_{prop}$).

d) Le premier bit se trouve encore sur la liaison entre les deux serveurs (position $= v \cdot d_{trans}$).

e) Le premier bit a déjà été reçu par le serveur B.

1.11 Imaginez que vous avez dressé Bernie, votre Saint-Bernard, pour qu'il transporte une boîte de trois cartouches à la place d'un tonnelet de whisky. Chaque cartouche contient 700 Mo de données. Bernie peut vous rejoindre où que vous soyez à une vitesse de 18 km/h. Pour quelle distance Bernie possède-t-il un débit plus élevé qu'une ligne de transmission à 10 Mb/s ?

Débit de Bernie : $B = 3 \cdot 700 \cdot 8 \cdot \frac{1}{\frac{d}{18 \cdot \frac{1000}{3600}}}$ Mb/s où d représente la distance cherchée.
On ne prend pas en compte le temps de propagation sur la ligne A à 10 Mb/s à moins que d se révèle très grand.
On cherche d tel que A = B :

$$10 = 3 \cdot 700 \cdot 8 \cdot \frac{1}{\frac{d}{18 \cdot \frac{1000}{3600}}} \Rightarrow d = \frac{16800 \cdot 5}{10} = 8400 \text{ m}$$

Bernie possède un débit plus élevé lorsque $d < 8400$ m.

1.12 Considérez un réseau LAN d'une distance maximale de 2 km. À quelle débit de transmission est-ce que le délai de propagation (vitesse de la lumière = 210'000 km/s) va être égal au délai de transmission pour des paquets de 100 octets ? Qu'en est-il pour des paquets de 512 octets ?

Délai de propagation : $d_{prop} = \frac{2 \text{ km}}{210'000 \text{ km/s}} = 9.524 \cdot 10^{-6} \text{ s} = 9.524 \ \mu\text{s}$

Débit x nécessaire pour transmettre 100 octets en $d_{prop} = 9.524 \cdot 10^{-6}$ s :
$9.524 \cdot 10^{-6} \text{ s} = \frac{100 \cdot 8 \text{ b}}{x} \Rightarrow x = \frac{800 \text{ b}}{9.524 \cdot 10^{-6} \text{ s}} = 84 \cdot 10^{6} \text{ b/s} = 84\text{Mb/s}$

Débit x nécessaire pour transmettre 512 octets en $d_{prop} = 9.524 \cdot 10^{-6}$ s :
$x = \frac{512 \cdot 8 \text{ b}}{9.524 \cdot 10^{-6} \text{ s}} = 430'080'000 \text{ b/s} = 430 \text{ Mb/s}$

1.13 Calculer le délai de tranfert (depuis le premier bit envoyé jusqu'au dernier bit reçu) pour les cas suivants :
a) Ethernet 10 Mb/s avec un seul commutateur de type « mémorisation et retransmission » (on attend que tout le paquet soit arrivé avant de le retransmettre sur la ligne) sur le chemin, et une longueur de paquets de 5'000 bits. Faites l'hypothèse que chaque ligne introduit un délai de propagation de 10 microsecondes et que le switch commence à retransmettre immédiatement après qu'il ait fini de recevoir le paquet.
b) La même chose avec trois switches.
c) La même chose mais on suppose que le switch implante un autre mécanisme : il est capable de commencer à transmettre le paquet après les 200 premiers bits qui ont déjà été reçus.

Considérons le schéma de la figure 1 qui représente le transfert du paquet.

a)
- Délai de propagation D_{prop} : 10 μs
- Délai de transmission D_{trans} : $D_{trans} = \frac{5 \cdot 10^3}{10^7} = 500 \ \mu s$
- Délai de transfert total : $D_{tot} = 2 \cdot D_{trans} + 2 \cdot D_{prop} = 1'020 \ \mu s$

b) Le principe est le même, il faut simplement ajouter deux switches dans le calcul précédent. Par conséquent, le délai de transfert total devient $D_{tot} = 4 \cdot D_{trans} + 4 \cdot D_{prop} = 2'040 \ \mu s$

c) Pour cette configuration, le délai de transfert total vaut $D_{tot} = 540 \ \mu s$

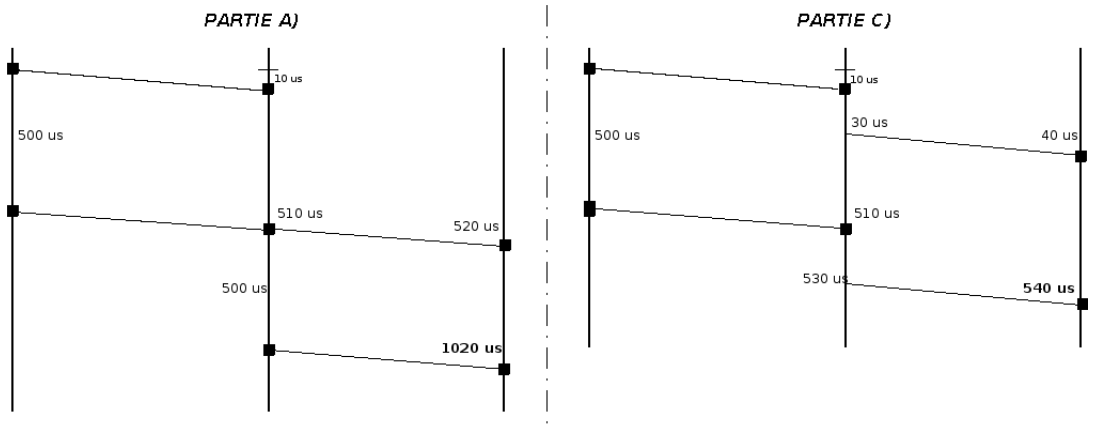


FIG. 1 – Illustration pour les partie a) et c) de la question 13

1.14 Un inconvénient des liaisons partagées est la perte de capacité lorsque plusieurs hôtes tentent d'accéder simultanément au canal. Prenons un exemple simple dans lequel le temps est divisé en intervalles discrets et où chacun des n hôtes tente avec un probabilité p d'accéder au canal durant chaque intervalle. Quelle est la proportion d'intervalles gaspillés en raison des collisions ?

X : Nombre d'hôtes qui accèdent simultanément au réseau

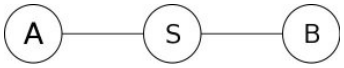
$X \sim \mathcal{B}(n, p)$

Binômiale car un utilisateur donné accède ou n'accède pas au réseau (Bernoulli) et qu'il y a n utilisateur(s) qui font cette expérience avec une probabilité de p.

On cherche $P(X \geq 2) = 1 - P(X < 2) = 1 - P(X = 0) - P(X = 1) =$
$1 - (1-p)^n - p \cdot (1-p)^{n-1}$.

1.15 Deux machines A et B sont connectées à un commutateur S via des lignes à 10Mb/s comme montré ci-dessous. Le délai de propagation sur chaque ligne est de 20 microsec. S mémorise et traite le paquet avant de le renvoyer sur la ligne. Il va le retransmettre sur la ligne 35 microsec. après avoir fini de le recevoir. Calculez le temps total requis pour transmettre 10000 bits de A à B quand
a) Un seul paquet est envoyé
b) Deux paquets de 5000 bits sont envoyés

a) – Longueur du paquet : $L = 10^4$ bits
– Délai de transmission (point-point) : $d_t = \frac{L}{d} = 2 * 10^{-3} = 1$ ms



- Temp de transmission total : $T_{tot} = 2 * d_t + d_{tr} + 2 * d_p = 2.075$ ms

b)
- Longueur de paquet : $L = 5 * 10^3$ bits
- Délai de transmission (point-point) : $d_t = 0.5$ ms
- Le second paquet suit directement le premier, on ne prend pas en compte pour lui les délais de propagation (qui n'influence que le premier bit transmit du premier paquet), ni le délai de traitement qui s'effectue pendant la transmission du premier paquet sur la seconde ligne, ni le délai de transmission sur la première ligne qui s'effectue pendant que le premier paquet est en cours de traitement sur le commutateur.
  On obtient donc : $T_{tot} = 3 * d_t + d_{tr} + 2 * d_p = 1.575$ ms

1.16 Qu'est-ce qu'une connexion ?

Une connexion est une liaison logique entre deux terminaux. Elle est associée à des paramètres qui sont négociés lors de l'établissement de la connexion. Les terminaux stockent ces paramètres pendant la durée de vie de la connexion, de telle manière qu'ils ne doivent pas être inclus dans tous les paquets transmis.

1.17 Pour quel type d'applications la commutation par datagrammes est préférable à l'établissement d'une connexion ?

- Pour des échanges très courts, comprenant très peu de paquets ;
- pour des applications multicast, dans lesquelles la même information est envoyée à plusieurs destinataires.

1.18 Calculez le temps total pour transférer un fichier de 1000 KB (K octets) dans les cas suivants, en faisant l'hypothèse que RTT = 100 ms, que la taille des paquets est 1 KB, et que 2 aller-retour (RTT) sont nécessaires pour l'établissement de la communication.
a) La largeur de bande est de 1.5 Mb/s, et les paquets sont envoyés de manière continue.
b) La largeur de bande est de 1.5 Mb/s, mais après chaque paquet on doit attendre 1 RTT avant d'envoyer le paquet suivant.
c) La largeur de bande est infinie, ce qui signifie que le temps de transmission est nul. On peut envoyer 20 paquets à la fois, par RTT.
d) La largeur de bande est infinie, et durant le premier RTT nous pouvons envoyer un paquet, durant le second RTT 2 paquets (22-1), durant le troisième RTT quatre paquets (23-1), et ainsi de suite. (Une justification sera donnée lorsque nous étudierons TCP).

Note : A voir avec le professeur, je n'arrive pas aux mêmes résultats que lui sur tous les calculs

- Délai de transmission : $d_{tr} = \frac{8 \cdot 10^3}{15 \cdot 10^5} = 5.333$ ms
- Nombre de paquets : $n = 1000$

a) $T_{tot} = 2.5 \cdot RTT + n \cdot d_{tr} = 250 + 5333 = 5583$ ms $= 5.583$ s

b) $T_{tot} = 2 \cdot RTT + (n-1) \cdot RTT + n \cdot d_{tr} = 200 + 99'900 + 5333 = 105'433$ ms $= 105.4$ s

c)
- Nombre de RTT nécessaire : $n_{rtt} = \frac{n}{20} = 50$
- $T_{tot} = 2 \cdot RTT + (n_{rtt} - \frac{1}{2}) \cdot RTT = 5100$ ms $= 5.1$ s

d)
- Nombre de RTT nécessaire : $n_{rtt} => n = \sum_{i=0}^{n_{rtt}+1} 2^i$
- Avec l'aide de la calculatrice, on arrive à : $n_{rtt} = \frac{ln(1001)}{ln(2)} = 9.96 \cong 10$

2 Modèles de référence

2.1 Décrivez en une phrase chacun des concepts entité, entité paire, protocole, service.

Entité Un élément actif du réseau.

Entité paire Un couple d'entités de la même couche qui communiquent entre elles.

Protocole Les règles et conventions de la communication entre entités paires.

Service L'ensemble des opérations (primitives) qu'une couche ou une entité fournit.

2.2 Nommez les couches du modèle de référence OSI en commençant par la couche la plus basse et indiquez pour chaque couche la fonction principale.

a) **Physique** : transmission de bits .

b) **Liaison** : découpage du flot de bits en trames, service fiable (contrôle d'erreurs, retransmission) ou non-fiable (détection d'erreurs, sans retransmission).

c) **Réseau** : interconnexion de sous-réseaux : adressage, routage, acheminement, fragmentation .

d) **Transport** : communication de bout en bout, service fiable (numéros de séquences, acquittements, retransmission, contrôle de flux, contrôle de congestion) ou non-fiable (démultiplexage vers la couche supérieure)

e) **Session** : services de session (p.ex. rattrapage après erreur).

f) **Présentation** : négociation de la syntaxe de transfert, traduction entre la syntaxe de transfert et la représentation utilisée par les systèmes terminaux.

g) **Application** : interface vers l'utilisateur.

2.3 Nommez 3 fonctionnalités de la couche Réseau (couche 3) du modèle OSI.

- Adressage des informations
- Routage des informations
- Acheminement de l'information
- Fragmentation

2.4 À quelle couche OSI correspond le protocole IP ?

À la couche réseau du modèle OSI.

2.5 Nommez 3 fonctionnalités de la couche Transport (couche 4) du modèle OSI.

- Contrôle d'erreurs (détection / correction d'erreurs) ;
- Retransmission
- Contrôle de flux
- Contrôle de congestion

2.6 À quelle couche OSI correspond le protocole TCP ?

Le protocole TCP correspond à la couche **transport** du modèle OSI.

2.7 Donnez des ressemblances et des différences entre les modèles OSI et Internet (DoD).
a) À quel niveau OSI fait-on le contrôle des erreurs de transmission (bits) ?
b) Et le contrôle des erreurs sur les paquets IP ?

Ressemblances : les fonctionnalités des couches OSI et celles utilisées dans Internet sont plus ou moins les mêmes.

Différences : la couche réseau du modèle OSI prévoit la possibilité de faire de l'orienté connexion tandis que ce qui est utilisé sur Internet n'est pas orienté connexion mais uniquement sans connexion (il faut dans chaque trame mettre la source et la destination).

a) Les erreurs de transmission sont contrôlées à la couche **liaison**.

b) Le contrôle des erreurs sur les paquets IP est effectué à la couche **transport**.

2.8 Expliquez la différence entre le contrôle de flux et le contrôle de congestion.

Le contrôle de flux adapte la vitesse de la transmission en fonction de la vitesse du récepteur d'un flux afin d'éviter de surcharger le récepteur. C'est une signalisation de bout-en-bout, dans laquelle le récepteur indique à l'émetteur la bonne vitesse de transmission.

Le contrôle de congestion adapte la vitesse de transmission à la capacité du réseau entre l'émetteur et le récepteur afin d'éviter de surcharger le réseau.

2.9 Quelle est la différence principale entre TCP et UDP ?

- TCP fournit un service de connexion fiable (contrôle de l'ordre des paquets et retransmission des paquets perdus/erronés).
- UDP fournit un service de connexion non-fiable.

2.10 Quel service est fourni par la couche IP du modèle TCP/IP ?

Le service fourni par la couche IP correspond au service fourni par la couche réseau du modèle OSI.

2.11 À quelle couche du modèle OSI travaille
a) un hub ?
b) un switch Ethernet ?
c) un routeur IP ?

a) hub = couche physique

b) switch = couche liaison des données

c) routeur IP = couche réseau

2.12 La retransmission de données peut se faire à la couche liaison et à la couche transport, mais la plupart des couches liaison (p.ex. Ethernet) ne fournissent pas de service fiable avec retransmission. Dans quelle situation est-il préférable d'effectuer les retransmissions déjà à la couche liaison ?

Si le taux d'erreurs bit est très élevé. Dans ce cas, beaucoup de trames contiennent des erreurs et il est plus efficace de les retransmettre à chaque lien.

2.13 Le taux d'erreurs bit sur un type de lien est de 10^{-6}.
a) Quelle est la probabilité qu'une trame de 1000 bits soit transmise correctement à travers un lien de ce type ?
b) Quelle est la probabilité que la trame soit transmise sans erreur sur 5 liens en de ce type en série ?

a) $\mathrm{P}(\text{trame correcte, 1 lien}) = (1-10^{-6})^{1000} = 1-1000\cdot 10^{-6} = 1-10^{-3} = 0.999 = 99.9\%$

b) $\mathrm{P}(\text{trame correcte, 5 liens}) = \mathrm{P}(\text{trame correcte, 1 lien})^5 = 0.995 = 99.5\%$

3 Médias de transmission

3.1 Soit un canal sans bruit de 4 kHz. Quel est le débit possible pour un signal binaire ?

Le débit binaire maximum d'un canal sans bruit peut être calculé avec le théorème de Nyqvist : $D_{max} = 2 \cdot H \cdot log_2(V)$

Dans notre cas, $H = 4$ kHz et $V = 2$, alors $D_{max} = 2 \cdot 4'000 \cdot log_2(2) = 8'000$ bit/s.

3.2 Les canaux de télévision ont une bande passante de 6 MHz. Quel est le débit binaire praticable pour une transmission à 4 moments ? Supposez que les canaux sont exempts d'erreurs.

À nouveau nous appliquons le théorème de Nyqvist, avec $H = 6$ MHz et $V = 4$ moments. Alors $D_{max} = 24$ Mb/s.

3.3 Quel débit binaire maximum peut-on obtenir avec un signal numérique envoyé sur un canal de 3 kHz dont le rapport signal sur bruit est de 20 dB ($= 10^2 = 100$) ?

La capacité du canal (alors le débit binaire maximum en présence de bruit) peut être calculé à l'aide de la formule de Shannon : $C = H \cdot log_2(1 + \frac{S}{N})$.

Dans notre cas, $H = 3$ kHz et $\frac{S}{N} = 20$ dB $= 100$. La capacité de ce canal est donc $C = 3'000 \cdot log_2(101) = 20$ kbit/s.

3.4 Quelle est la valeur du rapport signal sur bruit nécessaire pour transmettre le débit de 100 Mbit/s sur une ligne offrant une bande passante de 20 MHz ?

$C = 100$ Mbit/s, $H = 20$ MHz, alors $log_2(1 + \frac{S}{N}) = \frac{C}{H} = \frac{100 \cdot 10^6}{20 \cdot 10^6} = 5$.

$\Rightarrow \frac{S}{N} = 2^5 - 1 = 31$.

En décibel : $\frac{S}{N} = 10 \cdot log_{10}(31) = 14.9$ dB.

3.5 Qu'est-ce que la transmission en bande de base ?

La transmission de base n'effectue pas de transposition de fréquence. On émet alors un signal électrique dont la tension qui reflète directement les valeurs 0 et 1 des bits.

3.6 Expliquez pourquoi on doit utiliser un modem lors d'une transmission à longue distance.

Un modem transpose le signal de bande de base dans une bande de fréquence adaptée aux caractéristiques du support physique. Ainsi le signal modulé subit moins de distorsions et peut être transmis sur une distance plus grande.

3.7 Citez un avantage et un inconvénient d'une ligne non-équilibrée.

Avantage : Bon marché, comme il n'y a que peu de fils.

Inconvénient : Très sensible aux perturbation, donc débit et distance très limitées

3.8 Quel est l'avantage de torsader les fils d'une ligne équilibrée ?

Le fait de torsader les paires réduit les interférences électromagnétiques et améliore ainsi le débit et distance de transmission.

3.9 Quels sont les avantages et les inconvénients d'une fibre monomode par rapport à une fibre multimode ?

Avantages :
- débit maximum plus élevé ;
- permettent une distance de transmission plus longue.

Inconvénients :
- plus coûteuse ;
- nécessite une diode laser (coûteuse, courte durée de vie) comme source lumineuse.

3.10 Quelle bande de fréquences est utilisée par les systèmes modernes de transmissions de données tels que les réseaux LAN sans fils, les réseaux MAN sans fils et la téléphonie mobile ?

La bande de fréquence des micro-ondes, donc entre 100 MHz et 10 GHz.

Les réseaux LAN sans fils utilisent les fréquences de 2,4 GHz et de 5 GHz.

Les réseaux MAN sans fils utilisent des fréquences de 2 – 11 GHz.

Les réseaux de téléphonie mobile (GSM) utilisent plusieurs bandes de fréquences entre 900 MHz et 2 GHz.

4 La couche liaison

4.1 La couche liaison peut offrir un service fiable ou non fiable à la couche réseau. Dans quelle situation est-il plus avantageux de réaliser un service non fiable ?

Si le taux d'erreurs bit de la couche physique est très bas, on préfère mettre en œuvre un protocole de liaison très simple, donc non fiable. Dans ce cas, c'est la couche de transport qui doit effectuer la retransmission de paquets perdus ou erronés.

4.2 Quelle autre couche du modèle OSI peut effectuer la retransmission de données ?

La couche transport.

4.3 Quelles sont les deux fonctionnalités mises en œuvre par tous les protocoles de la couche liaison, même s'il n'offre qu'un service non fiable ?

Le découpage en trame et le contrôle d'erreurs (détections et suppression de trames erronées).

4.4 Si toutes les liaisons d'un réseau devaient procurer un service de transfert fiable, un service fiable à la couche transport serait-il complètement superflu ? Justifiez votre réponse.

Non, un service fiable à la couche transport est nécessaire même si toutes les liaisons du réseau sont fiables. Premièrement, un nœud intermédiaire peut subir une panne après avoir envoyé l'accusé de réception d'une trame. Dans ce cas, la trame est perdue mais elle ne sera pas retransmise à la couche liaison. Deuxièmement, il peut y avoir des erreurs bits (rafales d'erreurs très longues) qui ne sont pas détectées par la couche liaison.

4.5 Une chaîne de bits 0111101111101111110 doit être transmise par un protocole de liaison à découpage par fanion (01111110). Quelle est la chaîne transmise après l'ajout de bits de transparence ?

Le bit de transparence est le bit souligné.

$$\underbrace{01111110}_{\text{fanion}}0111101111\underline{\mathbf{0}}011111\underline{\mathbf{0}}10\underbrace{01111110}_{\text{fanion}}$$

4.6 Citez deux méthodes de découpages en trames.

- comptage de caractères : l'entête de trame indique la longueur de cette dernière (en comprenant l'entête) ;
- découpage orienté caractère : chaque trame commence par les séquences de caractères DLE STX (Data Link Escape, Start of TeXt) et termine par les séquences DLE ETX (End of TeXt) ;

– découpage à l'aide d'un fanion : chaque trame commence et termine par un fanion (01111110). Si dans la trame à transmettre, la couche détecte 5 bits à 1 à la suite, elle rajoute alors un 0 après le cinquième bit (cf question 5) ;
– découpage à l'aide d'une violation du codage physique ;
– période de silence entre les trames.

Remarque Certains protocoles utilisent la méthode du comptage de caractères plus une des trois autres.

4.7 Quel type d'erreurs pouvons-nous avoir sur un réseau informatique ? Qu'est-ce qui peut affecter une transmission correcte de l'information ? Comment y remédier pour obtenir une bonne fiabilité ?

Type d'erreur possible : erreurs sur 1 bit isolé, ou sur plusieurs bits à la suite (rafale d'erreur) plus facile à détecter, mais beaucoup plus dur à corriger.

Ce qui peut affecter une transmission : perturbations électromagnétiques pouvant se superposer au signal et donc fausser l'interprétation des données.

Comment y remédier : utiliser de la fibre optique qui propose une très bonne immunité aux perturbations. Sinon, il reste l'utilisation de codes détecteur/correcteur d'erreurs.

4.8 Citez deux codes correcteurs.

– parités horizontales et verticales ;
– code de Hamming (correction des erreurs simple ou double).

4.9 Citez deux codes détecteurs.

– code de parité ;
– code polynômial.

4.10 Pourquoi la plupart des protocoles fiables utilisent-ils un code détecteur avec une stratégie de retransmission plutôt qu'un code correcteur ?

Pour obtenir un code correcteur performant il faut ajouter beaucoup de bits aux trames envoyées. Vu le faible taux de perte des supports de transmission utilisés il est plus performant pour le débit d'ajouter un code détecteur qui utilise moins de bits plutôt qu'un code correcteur.

4.11 Pour obtenir une fiabilité supérieure à celle qu'offre un bit de parité unique, on veut utiliser un premier bit de parité calculé à partir des bits de rang impair et un second bit calculé à partir des bits de rang pair. Quelle est la distance de Hamming d'un tel code ? Justifiez votre réponse.

2, car si par exemple le premier et le troisième bit sont erronés le bit de parité associé ne pourra plus détecter les erreurs.

4.12 Essayez d'imaginer deux situations dans lesquelles un code correcteur (par exemple Hamming) est préférable à un code détecteur avec retransmission de trames.

- Un liaison simplex. Le récepteur ne peut pas signaler une erreur à l'émetteur.
- Une liaison à haut débit mais avec un délai de propagation très long (par exemple une liaison par satellite). Dans ce cas, la retransmission d'une trame prendrait beaucoup de temps et il serait préférable d'ajouter de la redondance pour pouvoir corriger les erreurs sans transmission.

4.13 Soit H la matrice génératrice d'un code Hamming et $\mathbf{G}^T$ la matrice de contrôle de parité.
a) Quelle est la formule (forme matricielle) pour calculer le mot de code y^T pour un vecteur de données x^T.
b) Quelle est la formule (forme matricielle) pour calculer le syndrome s^T pour un mode de code y^T.
c) Comment le syndrome est-il utilisé pour détecter une erreur ?

a) $y^T = x^T \cdot H$

b) $s^T = y^T \cdot G^T$

c) si le vecteur syndrome s^T est nul le mot de code est correct. Sinon, l'erreur est dans la ligne G^T correspondant à s^T.

4.14 La matrice génératrice H et la matrice de contrôle $\mathbf{G}^T$ d'un code de Hamming sont données plus bas.
a) Calculez le mot de code pour le vecteur de données x^T = (1001).
b) Est-ce que le mot de code y^T = 1100101 est correct ? Si non, quel bit doit être corrigé ?

Données $\mathrm{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$ $\mathrm{G}^T = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

4.15 Quelles erreurs sont détectables par un code polynomial de degré r ?

- toutes les erreurs simples ;
- toutes les erreurs doubles si le poynôme ne divise pas $x^k + 1$ pour $1 \leq k < n$ où n est la longueur de la trame ;
- toutes les erreurs sur un nombre impair de bits si le polynôme comporte $(x + 1)$ en facteur ;
- toutes les rafales d'erreurs d'au maximum r bits ;
- les rafales plus grandes que r bits avec une probabilité de $\frac{1}{2^{r-1}}$.

4.16 Considérez un code polynomial à 32 bits avec le polynôme générateur G(x). Nous voulons calculer le mot de code T(x) pour une séquence binaire M(x).

a) Pour quelle longueur de M(x) est-ce possible ?
b) Combien de bits de redondance sont ajoutés à une trame par ce code ?
c) Expliquez l'algorithme (forme algébrique) pour calculer le mot de code T(x) de M(x).
d) Expliquez l'algorithme (forme algébrique) pour vérifier si un mot de code T'(x) est correct.

a) Un code CRC est applicable à n'importe quelle séquence de données. Il permet donc de protéger des trames de longueur variable.

b) Un code CRC à 32 bits ajoute 32 bits de redondance à la séquence de données. Le nombre de bits de redondance est constant et ne dépend pas de la longueur de la trame.

c) Premièrement, on multiplie M(x) par x^{32}, ce qui correspond à un ajout de 32 fois 0 à la droite de M(x). Puis on divise $M(x) \cdot x^{32}$ par G(x). Cela donne un reste R(x). Le reste à une longueur de 32 bits. Le mot de code est alors donné par $T(x) = M(x) \cdot x^{32} + R(x)$, ce qui correspond à l'ajout de 32 bits de redondance à la droite de M(x).

d) Pour qu'un mot de code soit correct il doit être divisible par le polynôme générateur. On calcule donc T'(x)/G(x), et si le reste vaut 0 T'(x) est correct.

4.17 Supposez qu'un protocole utilise un code CRC à 16 bits. Quelle doit être la longueur des données pour que ce code soit applicable ?

Les codes CRC sont toujours appliquables peu importe la taille des données à transmettre.

4.18 Considérez le polynôme générateur CRC $x^3 + 1$.
a) Quelle est la séquence des coefficients binaires (4 bits) de ce polynôme ?
b) Considérez les bits de données 101010. Quel est le mot de codes à transmettre, y compris les bits de contrôle ? Montrez le calcul complet.
c) Quel est le mot de code pour les bits de données 101101 ? Montrez le calcul complet.

a) 1001

b) La division complète est représentée ci-dessous :

1	**0**	**1**	**0**	**1**	**0**	0	0	0	1	0	0	1
1	0	0	1									
0	0	1	1	1								
		1	1	1	0							
		1	0	0	1							
		0	1	1	1	0						
			1	0	0	1						
			0	1	1	1	0					
				1	0	0	1					
				0	1	1	1	0				
					1	0	0	1				
						1	1	1				

Vérification : $101111 \cdot 1001 + 111 = \mathbf{101010}000$ correct.

Le mot de code à transmettre est donc **101010**111.

c) La division complète est laissée comme exercice. Le mot de code à transmettre est **101101**000.

4.19 Est-ce que le mot de code 110110111 est correct si le polynôme générateur est $x^3 + x^2 + 1$? Montrez le calcul complet.

Les coefficients du polynôme sont 1101. Le mot de code est correct s'il est divisible par le polynôme générateur.

1	1	0	1	1	0	1	1	1	1	1	0	1
1	1	0	1									
0	0	0	0	1	0	1	1					
				1	1	0	1					
				0	1	1	0	1				
					1	1	0	1				
					0	0	0	0				

Le reste étant égal à zéro, le mot de code est correct.

4.20 Un mot de code a une longueur de 40 bits. Les bits 2, 5 et 10 ont été modifiés lors de la transmission. Quelle est la longueur de la rafale d'erreur ?

La rafale a une longueur de 9 (du bit 2 au bit 10 compris).

4.21 Les réseaux Ethernet utilisent un CRC à 32 bits. Quelle est la longueur maximum d'une rafale d'erreurs qui est détectée avec certitude ?

Les rafales de 32 bits sont toutes repérées, les rafales plus longues sont détectées avec un probabilité de 99,99999995 %.

4.22 Dans le protocole « Envoyer et attendre » (Stop-and-Go), combien de bits faut-il pour coder les numéros de séquence des trames et des acquittements ?

1 bit suffit.

4.23 Donnez un exemple d'un fonctionnement incorrect du protocole « Go-back-n » si la taille de la fenêtre est 4 et les numéros de séquence sont calculés modulo 4.

Un fonctionnement incorrect se produit lors de la situation suivante : un émetteur envoie 4 paquets, numérotés de 0 à 3. Le récepteur envoie les 4 acquittements, qui sont tous perdus. L'émetteur va donc retransmettre le paquet numéroté 0, cependant le récepteur attend le paquet 0 de la séquence suivante, donc il va recevoir des paquets à double sans pouvoir le détecter. C'est pourquoi il faut utiliser au minimum modulo (taille de la fenêtre + 1) numéros de séquence.

4.24 Dans un protocole utilisant une fenêtre glissante, comment faire pour dimensionner la taille de la fenêtre afin d'exploiter de manière optimale la capacité du réseau ? Donnez un exemple.

Afin d'obtenir une capacité optimale il faut utiliser comme taille de fenêtre le produit délai * largeur de bande.

4.25 Quelle est le produit largeur de bande * délai d'une fibre optique entre l'Europe et les États-Unis avec
- un délai de propagation 20 ms
- un débit de 10 Gb/s
- une longueur des paquets de données de 1500 octets
- une longueur des acquittements de 50 octets ?

$$\begin{aligned} RTT \cdot C &= L_{data} + L_{ack} + 2 \cdot D_{prop} \cdot C \\ &= (1500 \cdot 8 \text{ b}) + (50 \cdot 8 \text{ b}) + 2 \cdot 0.02 \text{ s} \cdot 10 \text{ Gb/s} = 400'021'400 \text{ bits} \end{aligned}$$

4.26 Quelle serait l'efficacité maximum (taux d'utilisation de la liaison) du protocole « Envoyer et attendre » sur cette liaison entre l'Europe et les États-Unis ?

$$\frac{L_{data}}{RTT \cdot C} = \frac{1'500 \cdot 8 \text{ b}}{400'012'400 \text{ b}} = 0.003\%$$

4.27 Un canal a un débit de 4 kb/s et un délai de propagation de 20 ms. On utilise un protocole du type « Envoyer et attendre » . Quelle taille de trame permet d'obtenir une utilisation du canal supérieure à 50 % ? Supposez que la taille des acquittements est 10 bits.

$$\frac{x}{x + 10 + 2 \cdot 0.02 \cdot 4 \cdot 10^3} > 0.5$$

$$\Rightarrow \quad x = 170 \text{ bits}$$

$$\Rightarrow \quad \text{multiple de } 8 : 22 \cdot 8 = 176$$

Trame de taille 22 octets.

5 Réseaux locaux

5.1 Soit un groupe de N stations partageant un canal à 56 kb/s selon le protocole ALOHA pur. Chaque station émet une trame de 1'000 bits à raison d'une toutes les 100 secondes, même si la trame précédente n'a pas pu être émise, chaque station gérant une file d'attente. Quelle est la valeur maximum de N ?

Le trafic généré par les stations ne peut pas être supérieur au trafic écoulé Y du système, sinon le système deviendrait instable. Le trafic écoulé Y dans ALOHA pur est de 0.184 Erlang au maximum, c'est-à-dire 18.4% de 56 kb/s = 10.3 kb/s.
Une seule station génère un trafic de $d = \frac{1'000 \text{ bits}}{100 \text{ s}} = 10$ bits/s. Pour ne pas dépasser le trafic écoulé :

$N \cdot 10 \text{ b/s} \leq 10'300 \text{ b/s} \Rightarrow N \leq 1'030$ stations

5.2 Dans les réseaux locaux, la couche liaison de données est divisée en deux sous-couches. Donnez leur nom et leurs fonctions principales.

Sous-couche LLC (Logical Link Control) : démultiplexage des trames vers les protocoles supérieurs.

Sous-couche MAC (Medium Access Control) : structurer le flot de bits en trames, gérer l'accès au médium, contrôle d'erreurs.

5.3 Quel type de service LLC utilisent les réseaux Ethernet ?

Ils utilisent la norme LLC 1 (sans acquittement et sans connexion).

5.4 Qu'est-ce qu'un domaine de collision ?

Ensemble des stations et systèmes intermédiaires d'un LAN dont les transmissions peuvent entrer en collision.

5.5 Dessinez le diagramme de flux de CSMA/CD.

Voir la figure 2 à la page 23.

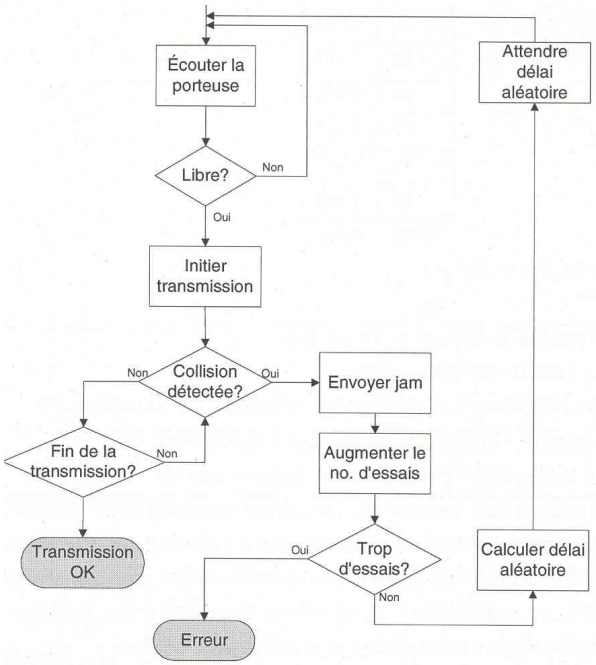


FIG. 2 – Ex 5 : diagramme de flux de CSMA/CD

5.6 Il existe trois variantes de l'algorithme CSMA. Laquelle est la base de la méthode CSMA/CD des réseaux Ethernet ?

CSMA-persistant.

5.7 Supposez que vous construisiez un réseau CSMA/CD fonctionnant à 1 Gb/s sur un câble de 1 km de long sans répéteur. La vitesse de propagation sur ce câble est de 200'000 km/s. Quelle doit être la taille minimale des trames sur ce réseau ?

- Délai aller-retour maximum : $RTT = \frac{2 \text{ km}}{200'000 \text{ km/s}} = 10 \ \mu s$
- Taille minimale des trames : $L = 1 \ \text{Gb/s} \cdot 10 \ \mu s = 10'000 \ \text{bits} = 1'250 \ \text{octets}$

5.8 Après avoir détecté une collision, une station émettrice doit attendre un délai aléatoire avant de retransmettre la trame. Le délai aléatoire est calculé selon la méthode « Truncated Exponential Backoff ». Supposons qu'une trame subisse 15 collisions consécutives et soit transmise avec succès lors de la 16 ème transmission. Combien de temps total la station a-t-elle dû attendre au maximum à cause du délai entre les retransmissions ?

Le délai aléatoire après n collisions est un multiple $r \cdot T$ de la fenêtre de collision T (51.2 μs), où r est un entier aléatoire uniformément distribué avec :

$$0 < r < 2^m - 1$$
$$m = \min(n, 10)$$

n	$\mathbf{r_{max}}$
1	1
2	3
3	7
4	15
5	31
6	63
7	127
8	255
9	511
10	1023
11	1023
12	1023
13	1023
14	1023
15	1023
Total	**7151**

Délai maximum : $7151 \cdot 51.2\ \mu s = 366$ ms

5.9 Nommez au moins 2 couches physiques (Base-. . .) des différents types d'Ethernet :
a) Ethernet 10 Mb/s
b) Ethernet 100 Mb/s
c) Ethernet 1000 Mb/s

a) 10Base-T, 10Base-2, 10Base-5

b) 100Base-TX, 100Base-FX

c) 1000Base-T, 1000Base-SX, 1000Base-LX, 1000Base-CX

5.10 Pour quels types de connexion faut-il utiliser un câble droit, pour quels types un câble croisé ?

- Câble droit : permet une connexion station – hub/switch ou une connexion routeur – hub/switch
- Câble croisé : permet une connexion hub/switch – hub/switch ou une connexion station – station

5.11 Pourquoi faut-il limiter la taille d'un domaine de collision en Ethernet ? Expliquez la relation avec l'algorithme de détection de collision.

Un émetteur Ethernet détecte une collision en comparant le signal émis avec le signal présent sur le canal. Il ne peut détecter une collision que s'il est en train d'émettre. Si la taille d'un domaine de collision est trop grande, le délai aller-retour d'un signal peut être plus grand que la taille de transmission d'une trame. Dans ce cas, il est possible qu'un émetteur ne détecte pas la collision d'une trame et la trame sera perdue.

5.12 Quelles sont les différences de la couche MAC entre 10Base-T et 100Base-TX ?

Il n'y a quasiment aucune différence entre la couche MAC de 10Base-T et de 100Base-TX. Comme le temps que dure un bit en 100Base-TX est dix fois moindre qu'en 10Base-T, le délai aller-retour est dix fois plus petit (5.12 μs) et la taille maximale d'un domaine de collision n'est plus que de 200 mètres. À part ça, toutes les fonctions de la couche MAC de 10Base-T sont conservées dans la couche MAC de 100Base-TX.

5.13 Quelles modifications ont été introduites dans la couche MAC 1000Base-TX par rapport à 100Base-TX ?

- *Carrier Extension* : ajoute des octets de bourrage pour augmenter le temps de transmission des trames et, de ce fait, augmenter la longueur maximale d'un segment ;
- *Frame Bursting* : cette option permet à une station de transmettre jusqu'à 5 trames de taille maximale sans donner la possibilité aux autres stations de transmettre.

5.14 À quoi sert l'extension de la porteuse (Carrier Extension) dans la couche MAC de Gigabit-Ethernet ? Dans quel mode de transmission est-elle applicable ?

Elle permet d'allonger la longueur maximale d'un segment.
Elle est applicable en mode half-duplex.

5.15 Imaginons que l'extension de la porteuse (Carrier Extension) n'ait pas été introduite dans Gigabit-Ethernet. Quelle serait la distance maximum possible entre deux stations liées par un segment UTP, si la vitesse de propagation du signal est de 200'000 km/s ?

La longueur minimale d'un paquet est de 64 octets = 512 bits
Le temps de transmission de cette trame en Gigabit-Ethernet est de : $T = \frac{512\text{b}}{10^9\text{b/s}} = 512$ ns.
Pour que la collision soit détectée, il faut que le RTT soit plus court que le temps de transmission :

$$RTT < 512 \text{ ns}$$

$$\frac{2 \cdot L}{200'000'000 \text{ m/s}} < 512 \cdot 10^{-9} \text{ s}$$

$$L < 51.2 \ m$$

5.16 Combien de paires contient un câble UTP ? Combien sont utilisées en 100Base-TX ? Combien sont utilisées en 1000Base-T ?

- Il contient 4 paires.
- 100Base-TX utilise 2 paires.
- 1000Base-T utilise les 4 paires.

5.17 Quelle catégorie de câble UTP faut-il pour Gigabit-Ethernet 1000Base-T ?

Des câbles de catégorie 5e ou 6.

5.18 Qu'est-ce qui se passe dans Ethernet lorsqu'une erreur bit (somme de contrôle incorrecte) est détectée ? Est-ce que la trame est retransmise par Ethernet ?

Lorsqu'une erreur bit est détectée dans une trame (avec le code polynomial CRC), la trame est simplement supprimée sur le récepteur. Cependant, Ethernet ne prévoit aucune retransmission des trames erronées, c'est donc au niveau de la couche supérieure qu'il manquera un paquet et qu'il sera retransmis.

5.19 Expliquez comment un émetteur détecte une collision dans Ethernet ?

L'émetteur écoute le canal pendant la transmission. Il compare le signal reçu avec le signal qu'il a émis. Si les deux signaux de correspondent pas, il y a eu une collision et l'émetteur envoie un signal de *jam* afin que la ou les autres machines qui émettent en même temps détectent aussi la collision.

5.20 Est-ce qu'une station qui ne transmet pas peut détecter une collision ?

Non elle ne peut pas.

5.21 Comment le destinataire d'une trame peut-il savoir que la trame a subi une collision et qu'elle est erronée ?

Le destinataire ne peut pas savoir s'il y a eu une collision, par contre lorsque les émetteurs détectent la collision, ils envoient un signal de *jam* qui va brouiller la fin de la trame. Ainsi la somme de contrôle sera erronée, car la trame sera trop courte et le destinataire écartera la trame.

5.22 Pourquoi la méthode CSMA/CD n'est-elle pas utilisée dans les réseaux locaux sans fil ?

Car la détection de collision n'est pas garantie, il est impossible d'écouter et de transmettre à la fois sur le médium.

5.23 Imaginez un bus Ethernet avec beaucoup de stations. Décrivez le comportement de ce réseau sous une charge très élevée ?

La probabilité que deux stations (ou plus) tentent de transmettre simultanément va augmenter rapidement. Le réseau Ethernet utilisant un protocole type CSMA/CD (Collision Detection), devra faire face à un très grand nombre de collisions sur son média déjà très occupé par les transmission qui passent correctement. À force, les backoffs vont devenir particulièrement long, diminuant les collisions, mais rallongeant grandement le délai d'accès au médium.

5.24 Quel effet peut-on observer lorsqu'un réseau Ethernet half-duplex (par exemple un bus) ne respecte pas la distance maximum entre deux stations ?

Comme la distance est trop grande, le délai aller-retour est plus grand que le temps de transmission d'une trame. Il est alors possible qu'une collision se produise et n'arrive à l'émetteur qu'après la fin de la transmission de sa trame. Comme il n'a pas détecté la collision, il considère que la trame est passée alors que ce n'est pas le cas. La trame est donc perdue.

5.25 Les trames Ethernet doivent comporter au minimum 64 octets pour que l'émetteur puisse détecter une collision avec fiabilité. Sur FastEthernet, la taille de trame minimale est identique, mais les bits sont expédiés dix fois plus vite. Comment est-il possible de maintenir la même taille de trame ?

Pour que les collisions soient détectées, il faut que les trames aient une taille minimale mais aussi que le domaine de collision soit plus court qu'une taille maximum fixée dans

la norme. Ces deux paramètres sont liés par la relation suivante :

$$RTT < d_{transmission} \Rightarrow$$
$$\frac{2 \cdot \text{Longueur maximale du domaine de collision}}{\text{Vitesse}} < \frac{\text{Taille minimale de la trame}}{\text{Débit}}$$

Ainsi, si on veut augmenter le débit sans augmenter la taille minimale des trames, il suffit de diminuer la longueur maximale du domaine de collision. Ainsi la fiabilité de la détection des collisions est maintenue.

5.26 Il existe deux formats de trames Ethernet : IEEE 802.3 et Ethernet-II.

a) Lequel des deux formats est utilisé par presque toutes les cartes réseau Ethernet et pourquoi est-il plus avantageux ?

b) Que se passe-t-il quand une carte réseau reçoit une trame dans l'autre format ?

a) Le format Ethernet-II, parce qu'il indique directement le type du protocole supérieur. Ainsi l'encapsulation LLC/SNAP n'est pas nécessaire et la trame est plus courte.

b) Chaque carte est capable de recevoir les deux formats mais n'en transmet qu'un seul.

5.27 Une trame IEEE 802.3 n'a pas de champs indiquant le protocole de la couche supérieure. Comment est-il possible de démultiplexer les trames reçues vers la couche supérieure ?

En utilisant l'encapsulation LLC/SNAP, qui contient un champ *type*.

5.28 La longueur maximum d'une trame Ethernet est de 64, 512, 1024 ou 1518 octets ?

1518 octets.

5.29 Quel est la fonction du protocole ARP ?

Le protocole ARP (Adress Resolution Protocol) permet de connaître l'adresse physique (MAC) d'une carte réseau correspondant à une adresse IP. Le protocole interroge (requête ARP) les diverses stations du réseau pour connaître leur adresse MAC et ainsi créer une table de correspondance entre les adresses logiques (IP) et les adresses physiques (MAC) dans une mémoire cache.

5.30 Indiquez les caractéristiques principales des adresses MAC

Elles sont formées de 48 bits, soit 6 bytes. (ex. : xx-xx-xx-xx-xx-xx, où « xx » représente 2 chiffres hexadécimaux ⇒ 1 octet). Chaque adresse MAC est unique. Les 6 premiers chiffres hexadécimaux d'une adresse MAC (les 3 premiers octets) sont attribués

au constructeur par l'IEEE. Les 6 derniers chiffres hexadécimaux (les 3 derniers octets) sont gérés par le constructeur.

Les adresses MAC sont encore divisées en deux catégories. Les adresses de groupe dont le premier bit est à 1 et les adresses individuelles dont le premier bit est à 0 (astuce : si la séquence hexadécimale la plus à gauche est impaire il s'agit d'une adresse de groupe). L'adresse de groupe la plus utilisée, appelée broadcast, a la forme suivante : FF-FF-FF-FF-FF-FF. Elle correspond à une adresse de diffusion générale.

5.31 Quelle est l'adresse MAC destinataire d'une trame de diffusion ?

L'adresse FF-FF-FF-FF-FF-FF (soit tous les bits à 1).

5.32 Comment les messages ARP sont-ils encapsulés ?

Les messages ARP sont encapsulés dans la partie données d'une trame Ethernet.

5.33 Pour les curieux :

On a deux stations qui veulent transmettre sur Ethernet. Chacune a une file d'attente avec des trames prêtes à être envoyées. Les trames de la station A sont numérotées A1, A2, ... et similairement pour les trames de la station B. L'unité de temps de backoff est de $T = 51.2\ \mu s$.

Supposez que A et B veulent envoyer simultanément leur première trame. Il y a une collision. Supposez que A choisit le délai aléatoire de $0 \cdot T$ et B de $1 \cdot T$. A va donc réémettre la trame A1 tout de suite et B attend son tour. Après cette transmission A va essayer de transmettre A2 et B va essayer de retransmettre B1. Il y a à nouveau une collision. Mais cette fois-ci A doit attendre un délai aléatoire de $0 \cdot T$ ou $1 \cdot T$, tandis que B doit attendre $0 \cdot T$, ..., $3 \cdot T$.

a) Donnez la probabilité que A gagne à nouveau après cette collision. C'est-à-dire, quelle est la probabilité que le délai aléatoire choisi par A soit plus petit que le délai aléatoire choisi par B.
b) Supposez que A choisit un backoff de $0 \cdot T$ et B de $1 \cdot T$. A gagne donc pour la seconde fois et va transmettre la trame A2. Ensuite A essayera de transmettre A3 et B la trame B1. Il y a de nouveau une collision. Donnez la probabilité que A gagne à nouveau et pourra transmettre la trame A3.

a) Voilà un schéma qui montre les tentatives de transmission dans le temps.

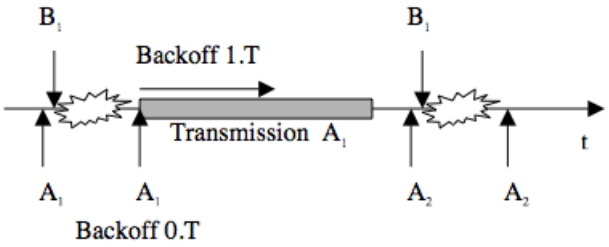


FIG. 3 – Corrigé 33 : Tentatives de transmission dans le temps

La probabilité que A gagne est donnée par

$$\begin{aligned} P(\text{A gagne}) &= 1 - (P(\text{Backoff}_\text{B} = 0 \cdot T) + P(\text{Backoff}_\text{A} = 1 \cdot T) \cdot P(\text{Backoff}_\text{B} = 1 \cdot T)) \\ &= 1 - \frac{1}{4} - \frac{1}{2} \cdot \frac{1}{4} \\ &= \frac{5}{8} \end{aligned}$$

Donc A gagne directement l'accès au canal avec une probabilité de 62.5%. À titre de comparaison, B gagne directement seulement dans 12.5% des cas (à savoir quand A calcule un backoff de 1 slot et B de 0 slot). Dans les autres cas (25%), il y a collision.

b) La probabilité que A gagne est donné par

$$\begin{aligned} P(\text{A gagne}) &= 1 - (P(\text{Backoff}_\text{B} = 0 \cdot T) + P(\text{Backoff}_\text{A} = 1 \cdot T) \cdot P(\text{Backoff}_\text{B} = 1 \cdot T)) \\ &= 1 - \frac{1}{8} - \frac{1}{2} \cdot \frac{1}{8} \\ &= \frac{13}{16} \end{aligned}$$

La probabilité que A gagne l'accès au bus augmente donc à chaque fois que B perd. Il est donc possible que A monopolise le canal. Cet effet est connu comme *l'effet de capture du canal* dans Ethernet.

5.34 La configuration 10Base-5 suivante est-elle permise si les noeuds intermédiaires sont des hubs ? Si non, corriger les erreurs.

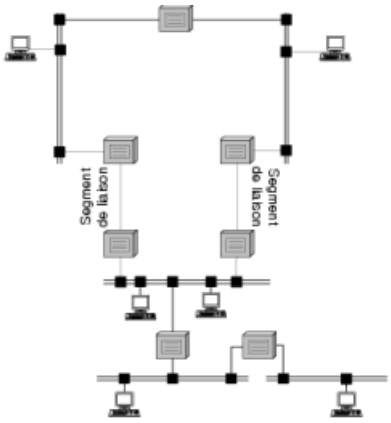


FIG. 4 – Schéma de la question 34

Non, car il est possible de former un chemin entre 2 stations qui passe par 5 répéteurs (alors que la limite est **4**). De plus ce chemin de taille maximum contient 6 segments (maximum **5**) (dont 5 sont des segments principaux alors que le maximum est de **3**). La correction à apporter est représentée à la figure 5 à la page 31.

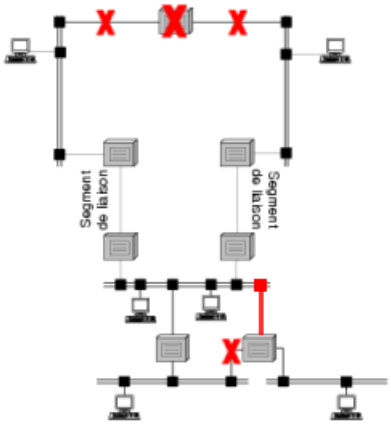


FIG. 5 – Schéma corrigé de la question 34

5.35 La configuration 10Base-5 suivante, est-elle permise,
a) si les noeuds intermédiaires sont des hubs ?
b) si les noeuds intermédiaires sont des switchs ?

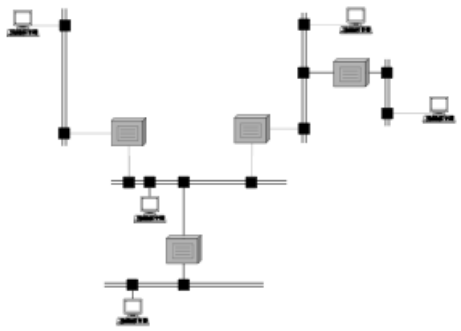


FIG. 6 – Exercice 35 : Configuration 10Base-5

a) Non, la configuration de respecte pas la règle 5-4-3-2-1 (il y a 5 segments principaux et le maximum est de 3).

b) Oui, les domaines de collision sont réduits aux segments principaux.

5.36 Comment pouvez-vous étendre la portée d'un réseau local ?

En utilisant des hubs et/ou un réseau commuté (avec des switchs).

5.37 Qu'est-ce qu'on utilise généralement pour séparer les domaines de collisions avec Ethernet : Répéteur, Hub, Switch, Pont, Routeur, . . . ?

En général, on utilise des switchs.

5.38 Quelles sont les différences entre
a) un répéteur et un hub ?
b) un hub et un commutateur ?

a) Un hub a plus d'interfaces qu'un répéteur mais leur fonctionnement est le même.

b) – Un hub travaille au niveau de la couche physique (niveau des bits), un commutateur au niveau de la couche liaison (niveau des trames).
– Un hub diffuse les trames reçues sur tous les ports de sortie. Un commutateur envoie les trames reçues seulement sur le port derrière lequel se trouve le destinataire.
– Un hub crée un seul domaine de collision. Un commutateur sépare les domaines de collision.

5.39 Quels sont les avantages et inconvénients d'Ethernet commuté par rapport à Ethernet partagé ?

Avantages :

1) Ethernet commuté augmente la largeur de bande disponible pour les stations.
2) Le filtrage des trames diminue le trafic dans le réseau et augmente la sécurité.
3) Ethernet commuté full-duplex permet des segments point à point sans limitation de longueur.

Inconvénients :

1) Un commutateur est plus cher qu'un hub ou un bus partagé.
2) Utilisation d'un contrôle de flux pour éviter la congestion du commutateur.

5.40 Quel serait l'effet si sur un segment Ethernet entre une station et un switch, une des interfaces est mise en Half-Duplex et l'autre en Full-Duplex ? Est-ce qu'il est possible de transmettre des trames à travers ce lien ?

Il est possible de transmettre des trames à travers ce lien, mais il y aura beaucoup de collisions comme l'interface Full-Duplex n'écoute pas le canal avant de transmettre.

5.41 Nommez 3 avantages de l'utilisation de switchs au lieu de hubs dans un réseau Ethernet.

- Le switch réduit le trafic dans le réseau comme le plus souvent une trame n'est transmise que sur une seule interface.
- Le switch augmente la sécurité du réseau comme les trames ne sont normalement pas diffusées à toutes les stations.
- La taille du réseau n'est pas limitée, le nombre de switchs à traverser entre deux stations n'est pas limité.

5.42 Quelles sont les fonctions principales d'un switch/bridge Ethernet ?

- Le filtrages des trames qui suivent ainsi un chemin entre l'émetteur et le destinataire.
- La création d'arbre de recouvrement pour éviter les boucles logiques et dévier le trafic d'un lien physique tombé.

5.43 Expliquez le terme « domaine de broadcast » dans le contexte d'un LAN switché

Dans le contexte d'un LAN switché, le domaine de broadcast est l'ensemble du réseau car les switchs diffusent des trames sur tous leurs ports actifs. Il s'agit donc de toutes les machines atteignables par une trame de diffusion, c'est-à-dire toutes les machines du même sous-réseau.

5.44 Pourquoi les LAN contiennent-ils souvent des boucles dans leur topologie physique ?

Cela crée une redondance et augmente la fiabilité du LAN en cas de panne d'un lien.

5.45 Pourquoi un LAN Ethernet ne fonctionne-t-il pas si la topologie contient une boucle ?

Lorsque le destinataire d'une trame est inconnu ou qu'une trame de diffusion est émise, la trame est diffusée sur le réseau entier et elle risque de circuler indéfiniment.

5.46 Quelles sont les trois étapes du protocole Spanning Tree ?

1. Élection de la racine.
2. Pour chaque switch : sélection d'un port racine.
3. Pour chaque LAN : sélection d'un port désigné.

5.47 Comment un administrateur de réseau peut-il influencer le choix de la racine de l'arbre recouvrant ?

En changeant la priorité attribuée à chacun des switchs.

5.48 Qu'est-ce que le port désigné d'un LAN ?

Le port vers un LAN qui offre le plus court chemin (le coût minimum) entre le LAN et la racine. Tous les autres ports qui permettent d'atteindre ce LAN sont désactivés.

5.49 Donnez un exemple qui montre comment le mauvais choix de la racine peut dégrader les performances du réseau.

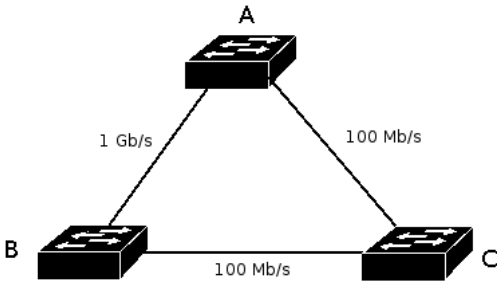


Fig. 7 – Réponse à l'exercice 49 : Mauvais choix de la racine

Si le switch C devient la racine de l'arbre recouvrant, le segment Gigabit-Ethernet entre A et B est désactivé et toutes les trames entre ces deux switchs traversent 2 segments à 100 Mb/s.

5.50 Décrivez les trois règles utilisées par les ponts transparents pour calculer le coût à l'aide des messages « Hello » (BPDU) ?

Selon les explications du labo LAN3, p.11, les règles de calcul du coût racine d'un port sont les suivantes :

- la racine émet des BPDU avec un coût égal à 0 ;
- chaque fois qu'un pont reçoit une BPDU, il copie le coût racine de la BPDU reçue comme coût racine du port de réception. Ensuite, il modifie le coût racine de la BPDU en ajoutant le coût local du port de réception. Il transmet cette BPDU modifiée sur tous les ports de sortie ;
- lorsqu'une BPDU est émise sur un port, le coût racine de la BPDU est copié comme coût racine du port.

5.51 Dans la configuration ci-dessous, calculez le coût racine de tous les ports si le coût local d'un port est 100.

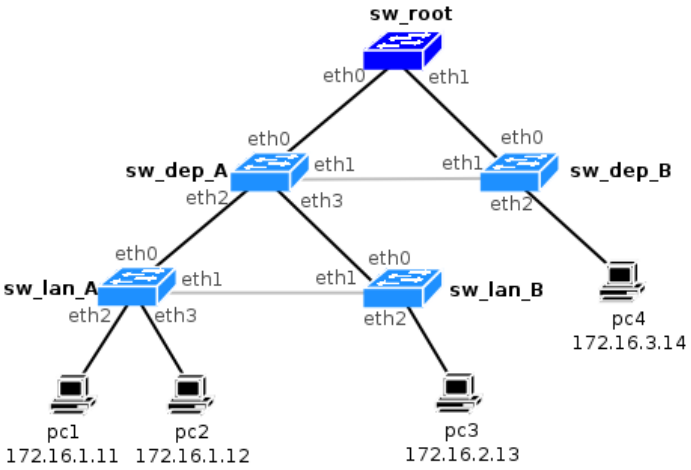


FIG. 8 – Réseau de l'exercice 51 (image tirée du labo LAN3)

Le coût racine de chaque port est donné dans le tableau suivant :

switch	*interface*	*coût*
sw_root	eth0	0
	eth1	0
sw_dep_A	eth0	0
	eth1	100
	eth2	100
	eth3	100
sw_dep_B	eth0	0
	eth1	100
	eth2	100
sw_lan_A	eth0	100
	eth1	200
	eth2	200
	eth3	200
sw_lan_B	eth0	100
	eth1	200
	eth2	200

Quelques remarques sur le calcul des coûts :

- **sw_root** : tous ses ports sont à un coût de 0 car c'est la racine ;
- **sw_dep_A** : eth0 a un coût de 0 à cause de la connexion directe à sw_root, les autres ports doivent ajouter 100 au coût du parcours jusqu'à la racine. Notons de plus que eth1 a normalement aussi recu un « Hello » venant de sw_dep_B qui avait un coût initial de 100 ;
- **sw_dep_B** : idem que sw_dep_A ;
- **sw_lan_A** : eth0 a un coût de 100 venant de l'interface eth2 de sw_dep_A ;
- **sw_lan_B** : eth0 a un coût de 100 venant de l'interface eth3 de sw_dep_A.

5.52 Dans le protocole STP, quel est le temps nécessaire à la reconfiguration après la panne d'un lien : 1 seconde, 12 secondes, 50 secondes, 2.5 minutes ?

50 secondes.

5.53 Dans la configuration ci-dessous, le port eth1 du switch sw_dep_A a été bloqué par STP. Le coût local de tous les ports est de 100. Sur quel port doit-on modifier le coût local pour réactiver le lien entre sw_dep_A et sw_dep_B et bloquer le lien entre la racine et sw_dep_B ?

Il n'est pas possible de désactiver les liens directs entre les switchs et la racine de l'arbre recouvrant.
La question est erronée, le prof va donc la supprimer du polycopié et elle ne sera pas dans le test.

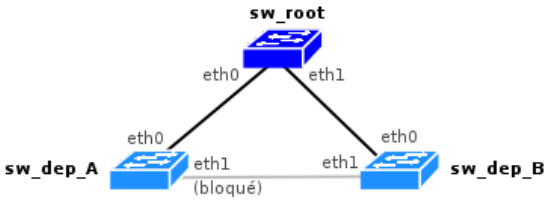


FIG. 9 – Réseau de l'exercice 53 (image tirée du labo LAN3)

5.54 Quels sont les trois avantages principaux de l'utilisation de VLAN dans un réseau local important ?

- chaque VLAN a son propre domaine de broadcast ce qui limite le nombre de trames de broadcast. Par conséquent cela limite le trafic du réseau ;
- les communications entre les VLAN peuvent être sécurisées par des firewalls ;
- les VLAN permettent d'affecter un utilisateur à un nouveau groupe sans recâblage (à la différence de deux sous-réseaux physiques).

5.55 Donnez un exemple d'une attaque qu'on peut prévenir à l'aide de VLAN.

Une attaque de type « Man-in-the-middle » puisque, à moins d'avoir un accès physique à un port du VLAN visé, l'attaquant ne pourra pas intercepter les paquets ARP depuis un autre VLAN.

5.56 Décrivez brièvement le principe des VLAN par port.

Chaque port est associé à un seul VLAN (excepté pour les ports *Trunk*) et les stations connectées sur un port font partie du VLAN.

5.57 Qu'est-ce qu'un trunk VLAN ?

Un lien entre deux switchs accédant chacun à deux ou plusieurs VLAN commun.

5.58 Quelle est la fonction du protocole 802.1Q (VLAN tagging) ?

Il sert à identifier le VLAN d'origine d'une trame. Il est utilisé uniquement entre les commutateurs.

5.59 Une école d'ingénieurs a deux VLAN : un VLAN 'professeurs' et un VLAN 'étudiants'. Comment est-il possible qu'un étudiant envoie un e-mail à un professeur ?

Afin de mettre en communication les différents VLAN il faut, comme pour deux réseaux physiques séparés, mettre en place un routeur.

5.60 Est-il possible d'utiliser un routeur avec une seule interface pour router entre plusieurs VLAN ?

Oui, le routeur est connecté à une interface trunk du switch et dispose d'une interface virtuelle pour chaque VLAN. Quand le routeur reçoit une trame, il enlève le VLAN tag et effectue l'algorithme de routage normal. Quand une trame est émise, l'interface virtuelle correspondante au VLAN marque la trame avec le VLAN tag correct.

5.61 Montrez une configuration dans laquelle un routeur, qui ne comprend pas l'encapsulation 802.1Q mais qui possède plusieurs interfaces réseau, peut router entre différents VLAN.

Chaque interface réseau du routeur est connectée sur le switch, et le switch attribue un VLAN différent pour chacun des ports connectés. De cette manière, le routeur fait partie de tous les VLAN. Il faut ensuite configurer correctement les règles de routage puis déclarer dans chaque VLAN l'adresse IP du routeur comme passerelle par défaut.

5.62 À une conférence, plusieurs participants aimeraient échanger des documents avec leur portable Wi-Fi. Il n'y a pas de point d'accès. Est-il possible d'établir un réseau WLAN ?

En utilisant le mode ad-hoc (transmission directe entre les stations).

5.63 Quels sont les débits maximum de IEEE 802.11a, 802.11b et 802.11g ?

802.11a : 54 Mb/s.
802.11b : 11 Mb/s.
802.11g : 54 Mb/s.

5.64 Quelles bandes de fréquences utilisent les normes 802.11 a, b et g ?

802.11a : 5 GHz.
802.11b : 2.4 GHz.
802.11g : 2.4 GHz.

5.65 En 802.11 b et g, combien de canaux sont utilisables simultanément sans interférence ?

802.11b : 3 canaux séparés.
802.11g : 3 canaux séparés.

5.66 Vous aimeriez installer un nouveau point d'accès 802.11g. Vous détectez la présence d'un autre point d'accès qui utilise le canal 4. Quel est le canal le plus bas que vous pouvez utiliser sans risquer des interférences avec le point d'accès voisin ?

Le canal 9.

5.67 Vous aimeriez installer un nouveau point d'accès 802.11g. Vous détectez la présence d'un autre point d'accès qui utilise le canal 4. Quel serait l'effet sur les performances de votre WLAN
a) si vous choisissez également le canal 4 ?
b) si vous choisissez le canal 5 ?

a) Si les deux AP utilisent le même canal, ils se partagent la bande passante. Comme chaque AP et station peut voir et interpréter les trames de l'autre cellule, tous les mécanismes du protocole 802.11 (p. ex. réservation du canal, respect des IFS) fonctionnent correctement.

b) Chaque AP voit les émissions de l'autre cellule comme du bruit qui cause des erreurs bit. Les AP ne peuvent pas correctement recevoir et interpréter les trames de l'autre cellule pour coordonner leurs actions. Il en résulte de très mauvaises performances.

5.68 Est-ce que des équipements 802.11b peuvent communiquer avec des équipements 802.11g ?

Oui, la norme 802.11g est compatible avec 802.11b.

5.69 Quels sont les avantages de 802.11g par rapport à 802.11a ? Quels sont les avantages de 802.11a ?

Avantages de 802.11g par rapport à 802.11a :
- bonne portée ;
- compatible avec 802.11b ;
- prix moyen.

Avantages de 802.11a :
- pas d'interférences avec d'autres équipements ;
- beaucoup de canaux utilisables simultanément.

5.70 La norme 802.11 définit deux méthodes d'accès au canal : DCF et PCF. Pourquoi ?

DCF est plus efficace pour la transmission de données sans contraintes temporelles.
PCF aurait dû permettre la transmission de service temps-réel, comme la voix et la vidéo. Or, il n'est pas implémenté dans les équipements actuels.

5.71 Décrivez brièvement le principe de l'évitement de collisions (la partie CA de CSMA/CA) de la couche MAC 802.11.

- une station écoute le canal avant de transmettre ;
- elle attend jusqu'a ce que le canal soit libre pendant un temps DIFS ;
- elle attend ensuite un délai aléatoire, calculé comme suit : time-slot * N, $N \in [0, CW]$ avec CW qui double à chaque collision jusqu'à la valeur CW_{max} ;
- transmission (si elle réussi, CW est remis a CW_{min}).

5.72 Dans le mode 802.11 sur infrastructure, une station A transmet une trame à une station B. Qui envoie un acquittement ?

Le point d'accès qui reçoit la trame envoie un acquittement à la station A. La station B, qui reçoit la trame depuis le point d'accès envoie ensuite un acquittement au point d'accès.

5.73 Expliquez pourquoi dans un mode sur infrastructure, une trame 802.11 est acquittée après chaque trajet, donc aussi par un AP intermédiaire. Quel serait l'inconvénient si l'acquittement était envoyé directement par le destinataire final à la source de la trame ?

Si le destinataire final doit acquitter la trame, le délai entre l'émission et la réception de la trame est variable, puisque le nœud intermédiaire n'a pas de garantie de pouvoir accéder au canal tout de suite. De ce fait, l'émetteur ne saura pas à partir de quand la trame doit être retransmise.

5.74 Dans quelles situations les différents intervalles 802.11 sont-ils utilisés :
a) DIFS
b) SIFS
c) PIFS

a) L'intervalle **DIFS** est utilisé au moment où une station veut entamer une nouvelle transmission sur le réseau.

b) L'intervalle **SIFS** est utilisé pour séparer les transmission au sein d'un dialogue (envoi de donnée, acquittement, etc...). Les deux autres intervalles se basent sur celle-la en y ajoutant un slot-time.

c) L'intervalle **PIFS** est utilisé uniquement par les points d'accès pour pouvoir émettre sur le réseau avec une priorité par rapport aux stations.

5.75 La norme 802.11 stipule que les intervalles de temps SIFS doivent avoir une durée inférieure aux intervalles de temps DIFS. Expliquez pourquoi.

De cette façon, aucune autre transmission ne peut intervenir entre la réception d'une trame et l'envoi de l'acquittement.

5.76 Comment une station 802.11 peut-elle détecter qu'une trame qu'elle a émise a subi une collision et qu'elle doit la retransmettre ?

Si elle ne reçoit pas d'acquittement en retour.

5.77 Après quels événements un émetteur 802.11 doit-il attendre un délai aléatoire ?

- si le canal était occupé lors de l'écoute ;
- après avoir transmis une trame ;
- après avoir détecté une collision.

5.78 Pourquoi un émetteur 802.11 doit-il attendre un délai aléatoire après avoir transmis une trame ?

Pour que chaque station ait toujours la même probabilité d'accéder au support. Effectivement, en imposant cette attente aléatoire, une station ne réserve jamais le support pour l'entier de sa connexion, mais se retrouve à demander l'accès au support pour chaque trame qu'elle désire transmettre.

5.79 Dans un réseau 802.11, A veut transmettre une trame à B à travers un point d'accès. Le point d'accès a reçu et acquitté la trame depuis A. Il doit la transmettre à B. Comment peut-il s'assurer qu'aucune autre station ne commence à transmettre avant lui ?

Il ne peut pas car il a la même priorité comme toutes les autres stations de la cellule.

5.80 La méthode CSMA/CA est basée sur CSMA persistant ou non-persistant ?

CSMA non-persistant, car une station ne transmet normalement pas quand le canal se libère. Elle doit encore attendre un délai aléatoire.

5.81 La méthode CSMA/CA permet d'éviter des collisions de manière très efficace. Quel est le défaut de cette méthode, au niveau des performances des transmissions ?

Le fait de « redemander » l'accès au support pour chaque transmission, et donc d'attendre un délai aléatoire à chaque trame, fait qu'on ne peut garantir un délai minimal pour la transmission d'une trame, compliquant ainsi la prise en charge d'applications temps réel comme la voix sur IP.

5.82 **Considérez un réseau 802.11b. Une station qui trouve le canal occupé lors de l'écoute doit attendre un délai aléatoire de $k \cdot$ *timeslot* où k est un entier aléatoire entre 0 et 31 et $timeslot = 20\ \mu s$.**
a) Quel est le nombre moyen d'essais avant de transmettre si le canal est occupé avec une probabilité de 80% ?
b) Quelle est la durée d'attente moyenne en état de backoff dans cette situation ?

a) 5 essais (le canal est libre avec une probabilité de 1/5).

b) $5 \cdot \frac{31}{2} \cdot 20\ \mu s = 1550\ \mu s$

5.83 **Une station d'un réseau 802.11b doit transférer un fichier à une deuxième station. Le réseau travaille en mode ad-hoc. Les autres stations sont silencieuses.**
Calculez le débit effectif de transmission de datagramme IP d'une taille de 800 octets chacun.
Procédez comme suit :
a) Dessinez un diagramme qui montre tous les délais de la transmission d'une trame (et l'acquittement). Les valeurs des différents délais IFS sont données dans la table 10.
b) Déterminez la taille d'une trame Wi-Fi à transmettre au niveau physique et la durée de transmission. Le format des trames MAC est montré à la figure 11.
c) Calculez le temps de transmission de l'acquittement. La longueur de l'acquittement est de 12 octets au niveau MAC.
d) Déterminez le débit effectif de la transmission de datagrammes IP en utilisant le délai total entre deux datagrammes et les données transmises dans cet intervalle de temps.

Intervalle / Norme	802.11	802.11a	802.11b
Slot time	$50\mu s$	$9\mu s$	$20\mu s$
SIFS	$28\mu s$	$16\mu s$	$10\mu s$
PIFS	$78\mu s$	$25\mu s$	$30\mu s$
DIFS	$128\mu s$	$34\mu s$	$50\mu s$

Fig. 10 – Délais de transmissions

Corrigé par le prof

5.84 **Quels sont les deux avantages de l'utilisation de la réservation du canal avec RTS/CTS ?**

– évite les collisions et retransmissions de trames très longues ;

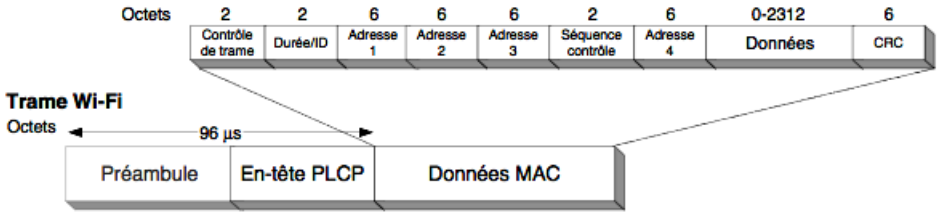


FIG. 11 – Format des trames Wi-Fi

– évite l'effet de la station cachée.

5.85 Supposez que les trames RTS et CTS de 802.11 soient d'une taille identique aux trames de données et acquittements normaux. Y a-t-il un avantage quelconque à avoir recours aux trames RTS et CTS ? Justifiez votre réponse.

Dans ce cas, l'utilisation de RTS et CTS n'a pas d'avantage, car la probabilité d'une collision d'un message RTS ou CTS est identique à celle d'une trame normale.

5.86 Le protocole WEP utilise comme base du cryptage des trames une clé composée d'une clé secrète partagée et d'un vecteur d'initialisation. Le vecteur d'initialisation n'est pas secret. À quoi sert-il ?

Le vecteur d'initialisation évite que plusieurs trames soient cryptées avec la même clé. De telles trames pourraient servir à un intrus afin de déchiffrer des trames.

Exemple La clé secrète partagée et le vecteur d'initialisation sont utilisés afin de générer une séquence d'octets pseudo-aléatoire :

$$S = RC4(Cl, IV).$$

Le cryptage est effectué à l'aide de l'opération exclusive-or entre le message M et la séquence pseudo-aléatoire :

$$C = M \oplus S.$$

Si l'intrus intercepte deux messages C_1 et C_2 cryptés avec le même vecteur d'initialisation, donc la même séquence pseudo-aléatoire, il peut effectuer l'opération suivante :

$$C_1 \oplus C_2 = M_1 \oplus S \oplus M_2 \oplus S = M_1 \oplus S \oplus S \oplus M_2 = M_1 \oplus M_2.$$

Il obtient donc l'exclusive-or des deux messages, **sans cryptage**. Cela peut être utilisé afin de deviner le contenu des deux messages. Cela fait, l'intrus peut déterminer la séquence pseudo-aléatoire S :

$$C_1 \oplus M_1 = M_1 \oplus S \oplus M_1 = M_1 \oplus M_1 \oplus S = S.$$

Cela lui permet de déchiffrer les autres trames chiffrées avec la même séquence S.

5.87 Après combien de temps le vecteur d'initialisation est-il réutilisé si on suppose la transmission d'une trame toutes les 2 ms ?

Le vecteur d'initialisation est codé sur 24 bits. Il y a donc $2^{24} = 16'777'216$ vecteurs différents. Les vecteurs d'initialisation sont réutilisés après la transmission de $16'777'216$ trames, donc après $16'777'216 \cdot 2$ ms = 9h et 20 minutes.

5.88 Actuellement, plusieurs protocoles de sécurité sont définis pour les réseaux 802.11. Lequel recommanderiez-vous
a) pour un réseau privé à la maison ?
b) pour le réseau d'un entreprise ?

a) WEP < WEP+ < WPA < WPA2

b) WPA < WPA2 et RADIUS, sinon VPN

5.89 Expliquez brièvement l'authentification et le contrôle d'accès avec le protocole 802.1X (serveur RADIUS).

- utiliser un serveur RADIUS pour authentifier chaque utilisateur ;
- l'accès au réseau reste bloqué jusqu'à l'authentification correcte ;
- authentification par un mot de passe, un certificat, une smart-card, ... ;
- création d'une clé de cryptage par session.

6 La couche réseau

6.1 Comment un destinataire sait-il qu'il a reçu le dernier fragment d'un datagramme fragmenté ?

Le bit M (« More fragments ») de l'en-tête IP du dernier fragment est mis à 0.

6.2 Lorsqu'un fragment a été perdu, que se passe-t-il au niveau du destinataire ?

Le destinataire supprime tous les fragments reçus. La couche supérieure (p.ex. TCP) doit éventuellement gérer la retransmission du paquet entier.

6.3 Nommez 3 fonctionnalités de la couche Réseau du modèle OSI.

- routage, acheminement ;
- adressage ;
- fragmentation.

6.4 IP effectue le réassemblage sur la machine de destination et non pas sur les routeurs intermédiaires. Pourquoi ?

Effectuer le réassemblage uniquement sur la machine de destination est plus performant que lorsqu'il doit être effectué sur les routeurs intermédiaires. En effet, les routeurs n'ont pas à stocker les fragments ni à effectuer un traitement dessus, comme il s'agit de paquets à part entière ils se chargent uniquement de les acheminer. De plus, les fragments peuvent emprunter des routes différentes donc un routeur peut ne pas avoir tous les fragments pour les réassembler.

6.5 Comment s'effectue un test ARP de doublons d'adresses IP ?

Lorsqu'un ordinateur se connecte à un réseau il effectue une requête ARP avec son adresse IP. S'il reçoit une réponse c'est qu'il y a un doublon d'adresse IP sur le réseau.

6.6 A quoi sert le champ TTL dans un datagramme IP ?

Le champ **durée de vie** (TTL : *Time To Live*) est un compteur utilisé pour limiter la durée de vie des datagrammes. Il est décrémenté à chaque saut (traversée d'un routeur). Le passage du compteur à la valeur zéro déclenche la destruction du datagramme et l'émission d'un datagramme d'avertissement à l'ordinateur source concerné. Cette routine limite la circulation de datagrammes parasites, qui se produit lorsque, par exemple, les tables de routage sont altérées.

6.7 A quoi sert le message ICMP de redirection ?

Le message ICMP de **redirection** apparaît lorsqu'un routeur détecte qu'un datagramme semble mal orienté. Ce message prévient l'ordinateur source d'une erreur probable.

6.8 Une station avec l'adresse IP 128.178.24.15 veut transmettre un datagramme au destinataire 212.10.12.20. Elle est configurée pour utiliser le routeur par défaut 128.178.24.1. Pour construire la trame MAC, elle envoie une requête ARP. Quelle adresse IP indique-t-elle dans la requête ARP ?

Celle du routeur : 128.178.24.1

6.9 Pourquoi utilise-t-on des adresses IP pour l'acheminement de paquets bien qu'on puisse identifier chaque interface à l'aide de son adresse MAC ?

Les adresses MAC ne permettent pas de regrouper les adresses pour former des réseaux. Il est donc impossible pour un routeur de savoir où se trouve un ordinateur avec une adresse MAC donnée. Les adresses IP par contre sont hiérarchiques, de telle manière qu'un routeur peut identifier le réseau auquel appartient une adresse et ainsi déterminer la route vers ce réseau.

6.10 Qu'est-ce qu'une adresse privée ? Donnez les plages d'adresses privées ? Dans quelles circonstances une organisation a-t-elle intérêt à utiliser des adresses privées ?

Une adresse privée n'est unique qu'à l'intérieur d'un réseau. Elle ne permet pas de transmettre des datagrammes à l'extérieur de ce réseau puisque plusieurs réseaux différents peuvent réutiliser les mêmes adresses IP. L'acheminement vers un destinataire avec une adresse privée est donc impossible dans le réseau global.

- Classe A : 1 réseau privé : 10.0.0.0 – 10.255.255.255
- Classe B : 16 réseaux privés : 172.16.0.0 – 172.31.255.255
- Classe C : 256 réseaux privés : 192.168.0.0 – 192.168.255.255

Une organisation peut utiliser des adresses privées si elle n'a pas de connexion à l'Internet global ou pour améliorer la sécurité, les ordinateurs avec une adresse privée n'étant pas visibles depuis l'extérieur.

6.11 Un réseau de classe B du réseau Internet définit plusieurs sous-réseaux ayant un masque de sous-réseau 255.255.240.0. Quel est le nombre maximum d'ordinateurs que l'on peut raccorder à chacun des sous-réseaux ?

255.255.240.0 = 1111 1111 . 1111 1111 . 1111 0000 . 0000 0000
Le NetId a une longueur de 20 bits, le HostId une longueur de 12 bits. Il peut donc y avoir $2^{12} = 4096$ adresse, ce qui donne 4094 ordinateurs (il ne faut pas compter l'adresse de réseau ni l'adresse de broadcast).

6.12 Parfois on utilise une autre notation pour les masques : Un masque de 25 bits signifie 255.255.255.128.
a) Trouvez l'adresse de diffusion (broadcast) de 172.30.0.141/25
b) Son adresse de sous-réseau.
c) Quelles sont les adresses valides au sein du même sous-réseau ?

Adresse IP	172.30.0.141	1010 1100.0001 1110.0000 0000.1000 1101
Masque	255.255.255.128	1111 1111.1111 1111.1111 1111.1000 0000

a) 172.30.0.255

b) 172.30.0.128

c) 172.30.0.129 à 172.30.0.254 (126 hôtes)

Explications : en appliquant l'opération logique ET de l'adresse IP et du masque de sous-réseau nous obtenons l'adresse du sous-réseau. À partir de cette adresse, en effectuant un OU logique sur l'inverse du masque de sous-réseau nous obtenons l'adresse de diffusion. Puis, pour calculer la plage possible il suffit, en se basant sur le format binaire de l'adresse de sous-réseau, de prendre l'ensemble des adresses possibles en modifiant les bits constituant l'adresse d'un hôte (en prenant soin de ne compter ni l'adresse de diffusion (*.*.*.255) ni l'adresse de réseau (*.*.*.0)).

6.13 Imaginez que votre machine veuille envoyer un paquet IP sur une machine étant dans le même sous-réseau que vous et que votre machine (10.10.10.1) ne connaisse que l'adresse IP de la destination (10.10.10.2). Quelles sont les messages qui seront échangés ?

La machine 10.10.10.1 va effectuer une requête ARP pour connaître l'adresse MAC de la machine 10.10.10.2. Une fois que l'autre machine aura répondu alors la transmission pourra commencer. Cependant les requêtes ARP ne sont pas tout le temps effectuées car il existe un cache sur les machines.

6.14 Quel masque de sous-réseau faut-il utiliser pour une adresse classe B si on veut avoir de sous-réseaux d'au maximum 1000 ordinateurs ?

Pour identifier 1000 ordinateurs il faut au minimum 10 bits ($2^{10} = 1024$). Le masque de sous-réseaux est donc 255.255.252.0.

6.15 Vous disposez de l'adresse réseau classe B 168.27.0.0. Proposez un masque de sous-réseaux qui vous permet de définir au moins 14 sous-réseaux disposant chacun d'au moins 2000 adresses hôte.

255.255.240.0 (4 bits pour le sous-réseau et 12 bits pour les hôtes) ou 255.255.248.0 (5 bits pour le sous-réseau et 11 bits pour les hôtes).

6.16 Vous disposez de l'adresse réseau classe A 10.0.0.0. Proposez un masque de sous-réseaux qui vous permet de définir au moins 500 sous-réseaux disposant chacun d'au moins 10'000 adresses hôte.

255.255.128.0 (9 bits pour le sous-réseau et 15 bits pour les hôtes) ou 255.255.192.0 (10 bits pour le sous-réseau et 14 bits pour les hôtes).

6.17 Supposez que l'adresse IP d'une interface est 128.12.34.71 et le masque de sous-réseau 255.255.240.0. Trouvez les valeurs suivantes :
a) ID de sous-réseau,
b) ID d'hôte,
c) Adresse de diffusion dirigée.

a) 128.12.32.0

b) 0.0.2.71

c) 128.12.47.255

6.18 Déterminez si les adresses IP suivantes sont des adresses spéciales, des adresses IP unicast, des adresses IP multicast ou des adresses invalides. Spécifiez aussi, le cas échéant, à quelle classe appartiennent ces adresses IP.
a) 33.0.0.45
b) 0.0.0.0
c) 255.255.255.255
d) 212.44.45.56
e) 100.78.189.1
f) 190.34.0.0
g) 10.255.255.255
h) 224.12.10.1
i) 127.0.0.1

a) 33.0.0.45 : adresse classe A d'un hôte

b) 0.0.0.0 : adresse « this host » ; adresse non définie

c) 255.255.255.255 : adresse de diffusion locale

d) 212.44.45.56 : adresse classe C d'un hôte

e) 100.78.189.1 : adresse classe A d'un hôte

f) 190.34.0.0 : adresse d'un réseau classe B

g) 10.255.255.255 : adresse de diffusion dans un réseau privé classe A

h) 224.12.10.1 : adresse multicast

i) 127.0.0.1 : adresse de rebouclage

6.19 Écrivez la classe et les éventuelles particularités des adresses IPV4 suivantes.
a) 129.127.13.2
b) 127.0.0.1
c) 222.223.224.255
d) 224.0.0.1
e) 192.168.24.10

a) 129.127.13.2 : adresse de classe B

b) 127.0.0.1 : adresse loopback

c) 222.223.224.255 : adresse de classe C, broadcast dirigé

d) 224.0.0.1 : adresse de multicast

e) 192.168.24.10 : adresse privée de classe C

6.20 Quelle adresse IP se trouve dans le même sous-réseau qui 130.12.127.231 si le masque de sous-réseau est 255.255.192.0 ?
a) 130.12.130.1
b) 130.22.130.1
c) 130.12.64.23
d) 130.12.167.127

l'adresse c) 130.12.64.23 est la seule dans le réseau 130.12.64.0/18.

6.21 Une organisation a un réseau de classe C 200.1.1.0 et désire créer des sous-réseaux pour quatre départements avec le nombre suivant de hosts : A : 72 hosts, B : 35 hosts, C : 20 hosts, D : 18 hosts. Ce qui donne 145 hosts en tout.
a) Donnez un arrangement possible des masques de sous-réseau pour accomplir cela.
b) Supposez que le département D grandit à 34 hosts. Que faites-vous ?

a) Le département A reçoit le masque de sous-réseau 255.255.255.128 et les adresses 200.1.1.1 à 200.1.1.126 (126 hosts).

Le département B reçoit le masque de sous-réseau 255.255.255.192 et les adresses 200.1.1.129 à 200.1.1.190 (62 hosts).
Le département C reçoit le masque de sous-réseau 255.255.255.224 et les adresses 200.1.1.193 à 200.1.1.223 (30 hosts).
Le département D reçoit le masque de sous-réseau 255.255.255.224 et les adresses 200.1.1.225 à 200.1.1.254 (30 hosts).

b) heu... j'suis dans la merde...

NOTE : cette question étant assez compliquée, elle ne sera pas dans les tests. De plus, l'approche choisie pour notre réponse est fausse, il faudrait en premier lieu partager le réseau 200.1.1.1 en deux sous-réseaux, chacun comportant à son tour deux sous-réseaux.

6.22 Supposez que l'adresse IP d'une interface est 10.192.73.201 et que le masque de sous-réseau est 255.255.240.0 Trouvez les valeurs suivantes :
a) Identificateur de sous-réseau
b) Identificateur
c) Adresse de diffusion dirigée

a) Identificateur de sous-réseau : 10.192.64.0

b) Identificateur d'hôte : 0.0.9.201

c) Adresse de diffusion dirigée : 10.192.79.255

6.23 Vous avez trouvé une place d'administrateur de réseau après vos études. Avant de vous envoyer faire une certification Cisco, on vous demande une recommandation pour l'adressage du réseau de votre entreprise. Jusqu'à présent, l'adressage de cette entreprise était constitué d'adresses publiques mais à cause de l'agrandissement de certains départements, on a décidé de passer à un adressage privé. Quelles recommandations allez-vous faire si une partie d'une entreprise comprend 5 entités : administration : 100 ordinateurs, développement hardware : 50 ordinateurs, développement software : 500 ordinateurs, recherche : 400 ordinateurs, marketing : 600 ordinateurs. On vous averti que le département du marketing risque de doubler d'ici deux ans. Quelles adresses allez-vous prendre ? Quels masques ? Quels sous-réseaux ? Quelles passerelles entre les différentes unités ? Quelle technologie ? Allez-vous utiliser des routeurs ? Si oui, lesquels ? quel genre de routage ? Donnez votre proposition.

Pour l'adressage du réseau nous allons nous baser sur la plage d'adresses privées 172.16.0.0 - 172.31.255.255 et utiliser l'adressage CIDR. La proposition pour les adressages est la suivante :

Département	sous-réseau	netmask	plage d'IPs	broadcast
administration	172.16.1.0/25	255.255.255.128	172.16.1.1 - 172.16.1.126	172.16.1.127
développement hardware	172.16.1.128/25	255.255.255.128	172.16.1.129 - 172.16.1.254	172.16.1.255
développement software	172.16.2.0/23	255.255.254.0	172.16.2.1 - 172.16.3.254	172.16.3.255
recherche	172.16.4.0/23	255.255.254.0	172.16.4.1 - 172.16.5.254	172.16.5.255
marketing	172.16.8.0/21	255.255.248.0	172.16.8.1 - 172.16.15.254	172.16.15.255

Pour le routage, nous proposons un routeur ayant une interface dans chaque sous-réseau et utilisant les adresses CIDR pour effectuer le routage.

6.24 Supposez que les hosts A et B sont connectés à un réseau Ethernet LAN avec une classe C d'adresses IP : 200.0.0.x. On veut ajouter un ordinateur C par une connexion directe sur B : voir figure 12. Expliquez comment nous pouvons faire cela avec les sous-réseaux. Donnez un exemple simple d'assignation de sous-réseau. Nous faisons l'hypothèse qu'aucune adresse supplémentaire n'est disponible. Qu'est-ce que ça implique sur la taille du réseau Ethernet ?

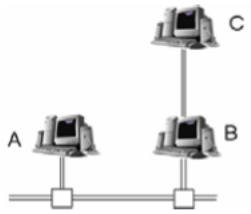


FIG. 12 – Réseau de l'exercice 24

La méthode pour connecter une machine C est d'utiliser un « proxy ARP » : B est d'accord de router le trafic vers C et de C. Il répond également aux requêtes ARP qui sont lancées sur le réseau Ethernet.

6.25 Quelles différences faites vous entre les notions de routage (« routing ») et de relayage (ou « forwarding ») ? Qui fait quoi ?

Routage : action de détermination de la route (le chemin) pour atteindre le destinataire. En pratique, cela consiste à déterminer l'interface de sortie et le noeud voisin.

Relayage : action de commutation d'une unité de transfert d'une interface en entrée vers une interface en sortie.

6.26 Quel est le problème principal des protocoles de routage par vecteur de distance ?

La convergence lente du protocole de routage. Lors d'une panne, la correction des tables de routage peut prendre beaucoup de temps.

6.27 Dans quelle situation un protocole de routage par vecteur de distance crée-t-il une boucle de routage ? Pensez à une topologie linéaire.

Regardez la figure suivante :

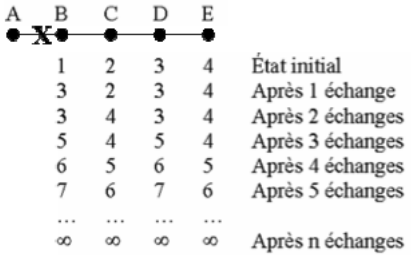


FIG. 13 – Figure de la solution de l'exercice 27

Lors de la panne du lien entre A et B, B reçoit encore des annonces de routes de C. Cependant, C calcule cette route à partir de l'annonce de route de B. Pendant cette phase de convergence, si B doit transmettre un datagramme à A, il l'achemine vers C. C l'achemine vers B et ainsi de suite.

6.28 Lequel des protocoles est utilisé pour le routage à l'intérieur d'un système autonome ?

a) OSPF
b) BGP

OSPF (Open Shortest Path First).

6.29 BGP est un protocole de routage

a) Par vecteur de distance
b) Par état de liaison
c) Les deux (a et b)
d) Aucun des deux (ni a ni b)

Réponse d), BGP est un protocole de routage particulier. Au lieu de maintenir le juste poids vers chaque destination, un routeur BGP garde la trace du chemin exact utilisé.

De même, au lieu de communiquer périodiquement à ses voisins son estimation des poids vers chaque destination possible, tout routeur indique à ses voisins le chemin exact qu'il utilise. Les chemins sont ensuite décidé par « accords commerciaux » entre les propriétaires des routeurs AS.

6.30 Deux routeurs peuvent-ils établir une boucle de routage en s'envoyant des messages BGP de mise à jour ?

Non. Les routeurs BGP échangent les routes complètes. Une boucle de routage peut facilement être détectée.

6.31 Expliquez les concepts de la remise directe et de la remise indirecte dans l'acheminement de paquets par un routeur.

Remise directe : Le routeur est connecté directement au réseau du destinataire d'un datagramme. Il peut donc directement envoyer une trame MAC au destinataire.

Remise indirecte : Le routeur n'est pas connecté au réseau du destinataire. Il doit envoyer le datagramme au prochain routeur qui le fait suivre vers le destinataire final.

6.32 Un routeur OSPF transmet des informations de routage
a) Uniquement à ses voisins directs
b) À tous les routeurs de sa zone

Réponse b), un routeur OSPF transmet des informations à tous les routeurs de sa zone.

6.33 Soit un routeur avec une interface 212.144.108.18 et un destinataire de 212.144.108.99. Y aura-t-il remise directe si l'on suppose que le réseau n'est pas mis en sous-réseau ?

Oui, le routeur et le destinataire sont directement connectés au même réseau C avec le NetId 212.144.108.00.

6.34 La table de routage d'un routeur avec une interface 100.3.4.3 contient les entrées suivantes ci-dessous.
Pour chacune des destinations suivantes, spécifiez s'il est possible de router vers la destination.
a) 221.3.4.1
b) 100.66.85.66
c) 199.22.1.9
d) 222.10.10.7
e) 222.0.44.44
f) 22.55.4.56

Destination	**Routeur de prochain pas**
100.0.0.0	Connexion directe
22.0.0.0	100.3.5.9
222.0.44.0	100.45.22.224
134.6.0.0	100.56.45.66
199.22.1.0	100.99.23.43

a) 221.3.4.1 : Non, pas de route vers le réseau de classe C 221.3.4.0

b) 100.66.85.66 : Oui, route vers le réseau de classe A 100.0.0.0

c) 199.22.1.9 : Oui, route vers le réseau de classe C 199.22.1.0

d) 222.10.10.7 : Non, pas de route vers le réseau de classe C 222.10.10.0

e) 222.0.44.44 : Oui, route vers le réseau de classe C 222.0.44.0

f) 22.55.4.56 : Oui, route vers le réseau de classe A 22.0.0.0

6.35 La table de routage d'un routeur RIPv1 contient les entrées du tableau ci-dessous.
Pour chacune des destinations suivantes, spécifiez s'il est possible de router vers la destination et si oui, le prochain pas.
a) 202.10.10.12
b) 201.12.5.28
c) 203.4.3.11
d) 202.10.10.33
e) 202.10.13.100

table de routage du routeur	
Destination	**Routeur de prochain pas**
200.1.1.0	Connexion directe
201.12.5.27	200.1.1.11
202.10.10.33	200.1.1.12
202.10.13.43	200.1.1.15
201.12.5.0	200.1.1.10
202.10.10.0	200.1.1.11
203.4.0.0	200.1.1.12

a) 202.10.10.12 : oui, le prochain pas est 200.1.1.11 ;

b) 201.12.5.28 : oui, le prochain pas est 201.1.1.10 ;

c) 203.4.3.11 : non cette adresse n'est pas routable ;

d) 202.10.10.33 : oui, le prochain pas est 200.1.1.12 ;

e) 202.10.13.100 : non cette adresse n'est pas routable.

6.36 Un routeur RIP contient les entrées du tableau ci-dessous dans sa table de routage.
La mise à jour RIP du second tableau est reçue en provenance du routeur voisin 145.108.1.9.
La métrique utilisée est le nombre de sauts. Quel est le nouveau contenu de la table de routage ? Quelle est la route par défaut ?

table de routage		
Destination	**Distance/coût**	**Routeur de prochain pas**
134.33.0.0	1	(directement connecté)
145.108.0.0	1	(directement connecté)
0.0.0.0	1	134.33.12.1
34.0.0.0	4	145.108.1.9
141.12.0.0	3	145.108.1.9

mise à jour RIP reçue de 145.108.1.9	
Destination	**Distance/coût**
199.245.180.0	3
34.0.0.0	2
141.12.0.0	4

La mise à jour des routes du routeur aboutit à la table de routage suivante :

table de routage après mise à jour		
Destination	**Distance**	**Prochain pas**
134.33.0.0	1	direct
145.108.0.0	1	direct
0.0.0.0	1	134.33.12.1
34.0.0.0	3	145.108.1.9
141.12.0.0	5	145.108.1.9
199.245.180.0	4	145.108.1.9

Route par défaut : 134.33.12.1

6.37 Utilisez l'algorithme de routage de Dijkstra pour trouver le plus court chemin entre A et F. Indiquez toutes les étapes intermédiaires.

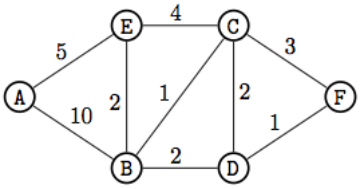


FIG. 14 – Réseau de l'exercice 37

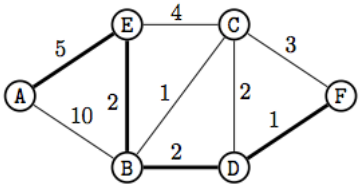


FIG. 15 – Solution de l'exercice 37

Détails de l'application de l'algorithme :

It.	Sommet	Couple (poids, préd.)						Liste
		A	B	C	D	E	F	
0		**(0,-)**	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	$\{A,B,C,D,E,F\}$
1	A	–	(10,A)	(∞,-)	(∞,-)	**(5,A)**	(∞,-)	$\{B,C,D,E,F\}$
2	E	–	**(7,E)**	(9,E)	(∞,-)	–	(∞,-)	$\{B,C,D,F\}$
3	B	–	–	**(8,B)**	(9,B)	–	(∞,-)	$\{C,D,F\}$
4	C	–	–	–	**(9,B)**	–	(11,C)	$\{D,F\}$
5	D	–	–	–	–	–	**(10,D)**	$\{F\}$

6.38 Utilisez la méthode qu'utilise OSPF (algorithme de Dijkstra) pour trouver les chemins les plus courts d'un nœud du réseau à l'ensemble des nœuds. Faites une matrice avec tous les nœuds et décrivez toutes les étapes. En particulier, quelle est la distance entre A et I ?

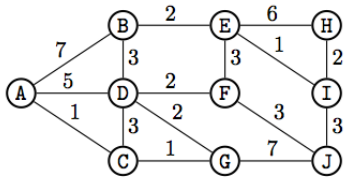


FIG. 16 – Réseau de l'exercice 38

Les plus courts chemins de A à tous les autres sommets du graphe sont donnés dans le tableau ci-dessous.

Sommet	Couple (poids, préd.)									
	A	B	C	D	E	F	G	H	I	J
	(0,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
A	–	(7,A)	**(1,A)**	(5,A)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
C	–	(7,A)	–	(4,C)	(∞,-)	(∞,-)	**(2,C)**	(∞,-)	(∞,-)	(∞,-)
G	–	(7,A)	–	**(4,C)**	(∞,-)	(∞,-)	–	(∞,-)	(∞,-)	(9,G)
D	–	(7,A)	–	–	(∞,-)	**(6,D)**	–	(∞,-)	(∞,-)	(9,G)
F	–	**(7,A)**	–	–	(9,F)	–	–	(∞,-)	(∞,-)	(9,G)
B	–	–	–	–	**(9,F)**	–	–	(∞,-)	(∞,-)	(9,G)
E	–	–	–	–	–	–	–	(15,E)	(10,E)	**(9,G)**
J	–	–	–	–	–	–	–	(15,E)	**(10,E)**	–
I	–	–	–	–	–	–	–	**(12,I)**	–	–

Le plus court chemin de A à I est 10, il est représenté en gras dans le graphe.

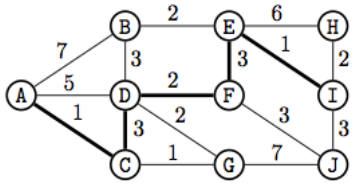


FIG. 17 – Solution de l'exercice 38

6.39 Trouvez à l'aide de l'algorithme de Djikstra le chemin le plus court entre Hobart (1) et Darwin (12). Les distances sont indiquées sur la carte de la figure 18.
ATTENTION : les liens sont directionnels !

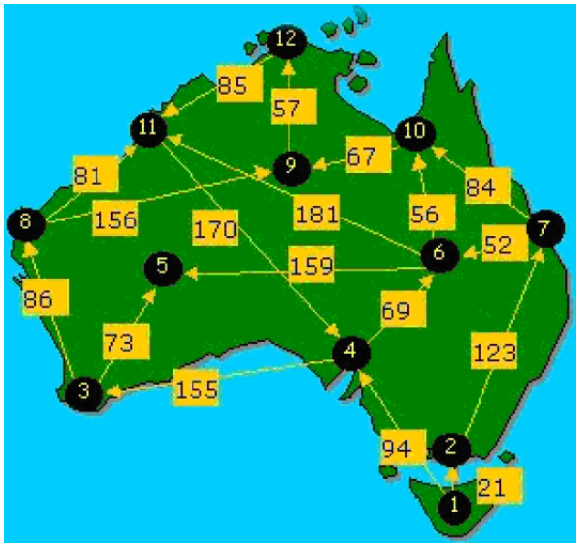


FIG. 18 – Réseau de l'exercice 39

Som.	Couple (poids, préd.)											
	1	2	3	4	5	6	7	8	9	10	11	12
–	**(0,-)**	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
1	–	**(21,1)**	(∞,-)	(94,1)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
2	–	–	(∞,-)	**(94,1)**	(∞,-)	(∞,-)	(144,2)	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
4	–	–	(249,4)	–	(∞,-)	(163,4)	**(144,2)**	(∞,-)	(∞,-)	(∞,-)	(∞,-)	(∞,-)
7	–	–	(249,4)	–	(∞,-)	**(163,4)**	–	(∞,-)	(∞,-)	(228,7)	(∞,-)	(∞,-)
6	–	–	(249,4)	–	(322,6)	–	–	(∞,-)	(∞,-)	**(219,6)**	(344,6)	(∞,-)
10	–	–	**(249,4)**	–	(322,6)	–	–	(∞,-)	(286,10)	–	(344,6)	(∞,-)
3	–	–	–	–	(322,6)	–	–	(335,3)	**(286,10)**	–	(344,6)	(∞,-)
9	–	–	–	–	**(322,6)**	–	–	(335,3)	–	–	(344,6)	(343,9)
5	–	–	–	–	–	–	–	**(335,3)**	–	–	(344,6)	(343,9)
8	–	–	–	–	–	–	–	–	–	–	(344,6)	**(343,9)**
9	–	–	–	–	–	–	–	–	–	–	(344,6)	–

Le plus court chemin de (1) à (12) passe par 1, 4, 6, 10, 9 et 12 avec une longueur de 343.

6.40 Quel est l'avantage principal de CIDR ?
a) CIDR utilise une fonction de hashage pour accélérer la recherche d'une route dans la table de routage.
b) CIDR réduit la taille des tables de routage.

Solution b), CIDR réduit la taille des tables de routage.

6.41 Adressage sans classes (CIDR) :
Le réseau d'une entreprise comprend 600 ordinateurs. Combien de blocs d'adresses de classe C doivent être alloués à l'entreprise (une adresse par ordinateur) ?
a) 1
b) 2
c) 3
d) 4

Il faut 4 adresses de classe C. En effet, pour pouvoir router le réseau de cette entreprise sans devoir ajouter 4 routes dans les routeurs il est nécessaire de créer un « super-réseau » comportant le même préfixe. Grâce à cela il est possible de n'ajouter qu'une seule route. Cependant, la contrainte est que le nombre de réseau doit être une puissance de deux. Ici, $2^{10} = 1024$ est le minimum nécessaire pour 600 ordinateurs.

6.42 Lorsqu'un routeur reçoit un paquet qu'il ne peut pas router, que se passe-t-il ?

Il le supprime et renvoie un message d'erreur ICMP « No route to host » à la source.

6.43 Un routeur a les trois interfaces 192.168.1.1, 192.168.2.1 et 192.168.3.1. Quelle est l'erreur dans sa table de routage représentée ci-dessous ?

Destination	Distance/coût	Routeur de prochain pas
192.168.1.0	1	(directement connecté)
192.168.2.0	1	(directement connecté)
192.168.3.0	1	(directement connecté)
192.168.4.0	2	192.168.1.2
192.168.5.0	3	192.168.4.2
192.168.6.0	4	192.168.2.2

Le routeur du prochain pas de la route 192.168.5.0 est impossible. Le routeur n'est pas connecté directement au réseau 192.168.4.0, donc il ne peut pas utiliser le routeur 192.168.4.2 comme routeur de prochain pas.

6.44 Montrez à l'aide d'un exemple comprenant 2 réseaux clients et un réseau ISP comment CIDR peut réduire la taille des tables de routage.

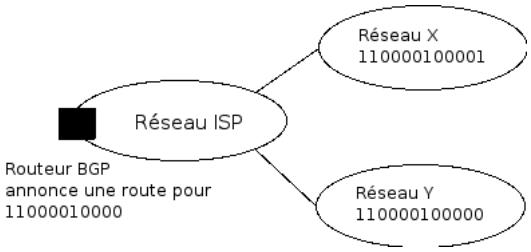


FIG. 19 – Réponse pour la question 44

6.45 Donnez un exemple d'un protocole de routage par vecteur de distance.

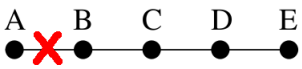
Le protocole RIP utilise la technique des vecteurs de distance.

6.46 Donnez un exemple d'un protocole EGP (Exterior Gateway Protocol).

BGP ou EGP.

6.47 Dans quelles circonstance RIP converge-t-il lentement ? Donnez un exemple.

RIP converge lentement lorsqu'un lien entre deux routeurs ne fonctionne plus. Un exemple est donné à la figure 20.



1	2	3	4	État initial
3	2	3	4	Après 1 échange
3	4	3	4	Après 2 échanges
5	4	5	4	Après 3 échanges
6	5	6	5	Après 4 échanges
7	6	7	6	Après 5 échanges
…	…	…	…	
∞	∞	∞	∞	Après n échanges

FIG. 20 – Exemple de convergence lente pour la question 47

6.48 Comment fonctionne le ”partage de l'horizon” ?

Le principe de l'horizon éclaté est le suivant : un routeur ne va pas annoncer de routes pour un réseau spécifique à son voisin si cette route passe effectivement par ce voisin. Par exemple, dans une chaîne de routeurs A - B - C, C ne va pas annoncer à B de route pour A car une telle route passe par B, par conséquent B connaît déjà une route pour aller vers A.

6.49 Les routeurs A et B sont des voisins comme montré à la figure 21 et ils utilisent RIP comme protocole de routage. Les tables de routage des routeurs A et B sont représenté dans les tableaux ci-dessous.

a) Quelles routes et distances A annonce-t-il à B, si l'horizon éclaté est désactivé ?

b) Quelles routes et distances A annonce-t-il à B, si l'horizon éclaté est activé ?

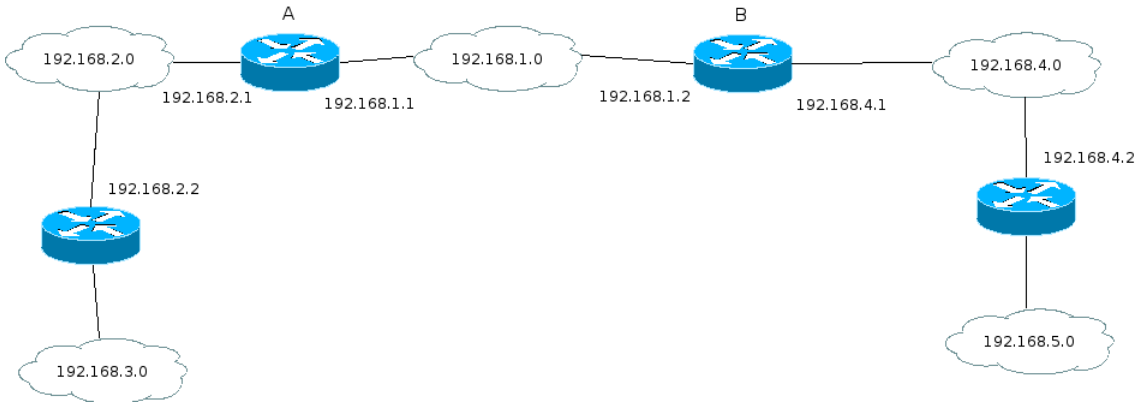


FIG. 21 – Réseau de la question 49

Table de routage du routeur A		
Destination	**Distance/coût**	**Routeur de prochain pas**
192.168.1.0	1	(directement connecté)
192.168.2.0	1	(directement connecté)
192.168.3.0	2	192.168.2.2
192.168.4.0	2	192.168.1.2
192.168.5.0	3	192.168.1.2

Table de routage du routeur B		
Destination	**Distance/coût**	**Routeur de prochain pas**
192.168.1.0	1	(directement connecté)
192.168.4.0	1	(directement connecté)
192.168.5.0	2	192.168.4.2
192.168.2.0	2	192.168.1.1
192.168.3.0	3	192.168.1.1

Les routes annoncées à B par le routeur A sont :

a) 192.168.2.0 (1), 192.168.3.0 (2), 192.168.4.0 (2), 192.168.5.0 (3)

b) 192.168.2.0 (1), 192.168.3.0 (2)

6.50 Les 6 routeurs (A,B,C,D,E,F) du réseau de la figure 22 ci-dessous utilisent un protocole de routage par état de liaison. Quel est le contenu du LSP (Link State Packet) envoyé par le routeur D ?

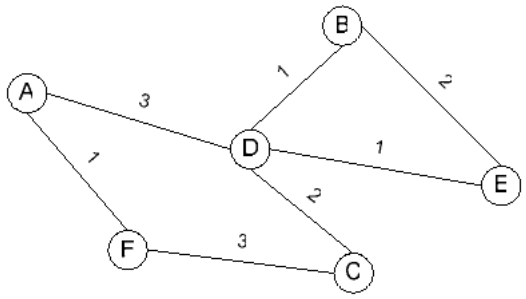


FIG. 22 – Réseau de la question 50

Le contenu du LSP envoyé par le routeur D est le suivant :

D	
A	3
B	1
C	2
E	1

6.51 Indiquez les particularités des adresses suivantes :

a) $FF01:0:0:0:0:0:0:101$

b) $::1$

c) $1080::A110:123::FE02$

d) $FE80::0A10:FCFF:FE32:A802$

e) $0:0:0:0:0:0:13.1.68.3$

a) $FF01:0:0:0:0:0:0:101 \rightsquigarrow$ Adresse multicast

b) $::1 \rightsquigarrow$ Adresse de rebouclage

c) $1080::A110:123::FE02 \rightsquigarrow$ Notation incorrecte (deux fois "::")

d) $FE80::0A10:FCFF:FE32:A802 \rightsquigarrow$ Adresse locale du lien

e) $0:0:0:0:0:0:13.1.68.3 \rightsquigarrow$ Adresse IPv6 compatible IPv4

6.52 Lors de la configuration automatique sans état dans IPv6, une station construit une adresse locale de lien afin de pouvoir communiquer avec les routeurs connectés au lien. Décrivez le mécanisme utilisé par la station pour s'assurer que cette adresse locale n'est pas utilisée par une autre station.

Elle envoie un message "Sollicitation de voisins" à toutes les machines du lien avec l'adresse qu'elle vient de construire. S'il n'a pas de réponse, elle est seule à utiliser cette adresse.

6.53 Le champ "Protocol" de l'en-tête de datagrammes IPv4 n'est pas présent dans l'en-tête IPv6. Pourquoi ?

Il est remplacé par le champ 'En-tête suivant' dans l'en-tête IPv6. Ce champ va indiquer s'il y a un en-tête d'extension ou si la suite du paquet est un datagramme pour une couche supérieure.

6.54 Expliquez le mécanisme de résolution d'adresses MAC (fonctionnalité du protocole ARP dans IPv4) dans IPv6.

Un hôte envoie un message "Sollicitation de voisin" à l'adresse multicast "Tous les nœuds de son réseau". Il indique l'adresse IPv6 du nœud cherché. Le nœud cherche répond avec un message ICMPv6 "Annonce d'un voisin" destiné au premier hôte. Ce message contient l'adresse MAC du nœud.

6.55 Dans IPv6, le routage par la source est plus efficace que dans IPv4 parce que
a) L'en-tête IP a été simplifié ;
b) Seuls les routeurs concernés examinent l'en-tête d'extension de routage par la source.

b) Seuls les routeurs concernés examinent l'entête d'extension de routage par la source. En effet, avec IPv6 l'adresse de destinataire correspond au prochain routeur dans la liste de routage par la source. Lorsqu'un routeur reçoit un tel paquet, il consulte l'entête d'extension pour trouver l'adresse du prochain routeur et la met à la place de l'adresse du destinataire. La dernière adresse dans la liste correspond à l'adresse de destination.

6.56 Dans IPv6, que fait un routeur lorsqu'il reçoit un datagramme qui est plus long que la MTU de l'interface de sortie ?
a) Il fragmente le datagramme ;
b) Il supprime le datagramme et envoie un message d'erreur à la source.

b) Il supprime le datagramme et envoie un message d'erreur ICMPv6 « Paquet trop grand » à la source.

6.57 Dans IP Mobile, l'agent domestique doit intercepter tous les messages destinés à un nœud mobile lorsque celui ne se trouve pas dans son réseau d'origine. Expliquez le mécanisme utilisé par l'agent domestique.

L'agent domestique utilise la technique proxy-ARP. Il répond aux requêtes ARP concernant l'adresse IP du nœud mobile avec sa propre adresse MAC. Ainsi, toutes les trames MAC destinées au nœud mobile sont redirigées vers l'agent domestique.

7 Sécurité sur Internet

Pas à l'examen.

8 La couche transport

8.1 Quelles sont les principales analogies entre la couche transport et la couche liaison ? Quelles en sont les principales différences ?

Analogies : les deux couches peuvent fournir un service fiable ou non.

Différences : la communication se fait de bout en bout pour la couche transport, et elle connait le délai aller-retour.

8.2 TCP et UDP sont des protocoles qui travaillent sur
a) les routeurs
b) les switches
c) les systèmes terminaux (PCs et serveurs)
d) tous les nœuds du réseau ?

Réponse c), les protocoles TCP et UDP travaillent uniquement sur les systèmes terminaux.

8.3 Dans quel intervalle les numéros de port TCP et UDP sont-ils pris ? Les numéros de port TCP sont-ils indépendants des numéros UDP ?

Les numéros de ports sont des entiers codé sur 16 bits. Ils peuvent donc prendre les valeurs entre 0 et 65'535.
Oui, ils sont indépendants, sur la même machine, un service peut écouter le port 3003 de TCP pendant qu'un autre écoute ce même numéro de port mais d'UDP.

8.4 Quelles sont les fonctions mises en œuvre par TCP ? Nommez-en au moins 4 !

- transmission fiable ;
- contrôle de flux entre les systèmes terminaux ;
- contrôle de congestion du réseau ;
- possibilité de retransmission ;
- utilisation d'acquittements.

8.5 Expliquer brièvement la différence entre les ports bien connus et les ports éphémères. Dans quelles situations respectives sont-ils utilisés ?

Un port bien connu est assigné de manière fixe à un service. Un serveur comme ftp ou http écoute à ce port et peut ainsi facilement être contacté par un client. Un port éphémère est assigné de manière temporaire à un client ou un service moins important. Il peut être réutilisé par d'autres applications.

8.6 Pourquoi UDP existe-t-il ? Est-ce qu'on n'aurait pas pu se contenter de laisser les utilisateurs envoyer leurs paquets IP bruts ?

UDP est nécessaire pour démultiplexer les paquets reçus par la couche réseau. Le numéro de port de destinataire sert à identifier l'application qui doit recevoir le paquet.

8.7 Pour quels types d'applications faut-il utiliser UDP plutôt que TCP ? Donnez trois types d'applications.

- les services multimédia, qui peuvent tolérer des pertes de paquets ;
- les transmissions multicast, TCP ne supportant pas le multicast ;
- les échanges très courts de messages (comme DNS) où l'établissement d'une connexion serait trop lent.

8.8 TCP est un protocole de transport visant à offrir des communications de bout en bout fiables. Quels mécanismes de communication met-il en œuvre pour cela ? Autrement dit, si on suppose que le réseau sous-jacent est fiable, quelles sont les fonctionnalités de TCP qui deviennent inutiles ?

Les éléments du service fiable de TCP sont
- les numéros de séquence ;
- les acquittements ;
- la retransmission.

Par contre, le contrôle de flux et le contrôle de congestion seraient nécessaires même si la couche réseau était fiable.

8.9 Pourquoi ne pas commencer la numérotation de séquence toujours à 0 ?

Pour diminuer le risque que des doublons soient pris pour des segments valables.

8.10 Décrivez brièvement le rôle du flag TCP PSH (push).

Le drapeau push permet de forcer TCP à transmettre toutes les données précédemment contenues dans son tampon au destinataire.

8.11 Décrivez brièvement le rôle du flag TCP URG (urgent).

Le drapeau urgent indique au récepteur qu'il y a des données urgentes et qu'il ne doit pas traîter l'ensemble des données du tampon de réception mais traiter directement les données urgentes.

8.12 Quel est le rôle de l'option MSS de TCP ?

l'option MSS (Maximum Segment Size) permet de spécifier la charge utile la plus grande qu'un récepteur peut recevoir. Elle permet de négocier la taille maximale d'un segment TCP.

8.13 Quels sont les avantages et désavantages du caractère cumulatif des acquittements TCP ?

Avantages :
- il n'est pas nécessaire d'acquitter chaque segment séparément ;
- un acquittement perdu n'implique pas nécessairement une retransmission.

Inconvénients :
- si un segment intermédiaire a été perdu, le récepteur ne peut pas signaler la réception correcte des segments suivants ;
- l'émetteur retransmettra probablement tous les segments à partir du segment perdu (méthode Go-back-n).

8.14 Qu'est-ce que la négociation en trois temps de TCP ? Expliquez-en les trois phases.

Cette négociation en trois temps est utilisée lors de l'ouverture d'une connexion. Elle permet aux deux hôtes de préparer la transmission des données et de se mettre d'accord sur les numéros de séquences. Elle se passe comme suit :

1) A envoie un paquet SYN avec un numéro de séquence x, les ports source et destination
2) B répond à A avec un paquet SYN ACK, le SYN contenant un numéro de séquence aléatoire, le ACK demandant le paquet avec le prochain numéro de séquence à A.
3) A répond à B avec un ACK pour demander le paquet avec le numéro de séquence suivant à B.

8.15 Pourquoi procéder à un échange en trois phases lors de l'établissement d'une connexion ?

L'établissement de connexion en trois phases a deux fonctions :
- les hôtes se mettent d'accord sur les numéros de séquence initiaux ;
- il diminue le risque qu'un doublon d'un segment SYN conduit à l'établissement d'une connexion.

8.16 Le diagramme ci-dessous, montrant la libération d'une connexion, est-il correcte ? Si non, corriger l'erreur.

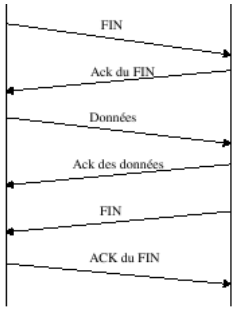


FIG. 23 – Libération d'une connexion de l'exercice 16

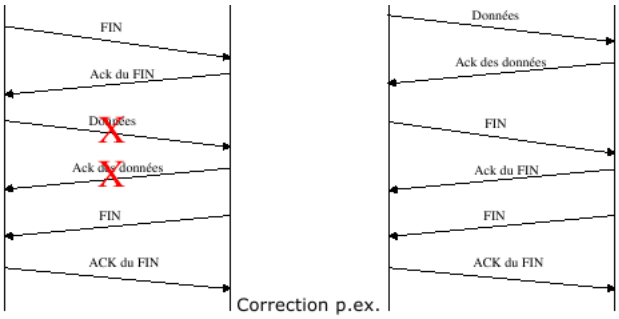


FIG. 24 – Réponse de l'exercice 16

8.17 **L'échange TCP de la figure 25 correspond au transfert d'une page WEB entre un navigateur WEB et un serveur WEB. On fait l'hypothèse que la requête à la page WEB fait 100 octets et que la page WEB retournée fait 1'000 octets. Il n'y a pas d'erreurs de transmission. Pour chaque segment de données, différentes informations apparaissent. D'une part la présence d'un ou plusieurs des différents indicateurs comme SYN, FIN, ACK. Par ailleurs sur la première ligne deux chiffres sont portés. Le premier chiffre correspond au numéro de séquence du premier octet du segment, le deuxième chiffre correspond au numéro du premier octet du prochain segment à envoyer. Le chiffre entre parenthèses correspond au nombre total d'octets transmis dans le segment. Si le segment est porteur d'un acquittement positif, l'indicateur ACK est mentionné et a coté de lui doit figurer la valeur du champ acquittement du segment TCP.**
Complétez les numéros de séquence et les numéros d'acquittement qui manquent sur la figure (qui apparaissent sous forme de point d'interrogation). Indiquez à quoi correspondent les différents segments numérotés de 1 à 8.

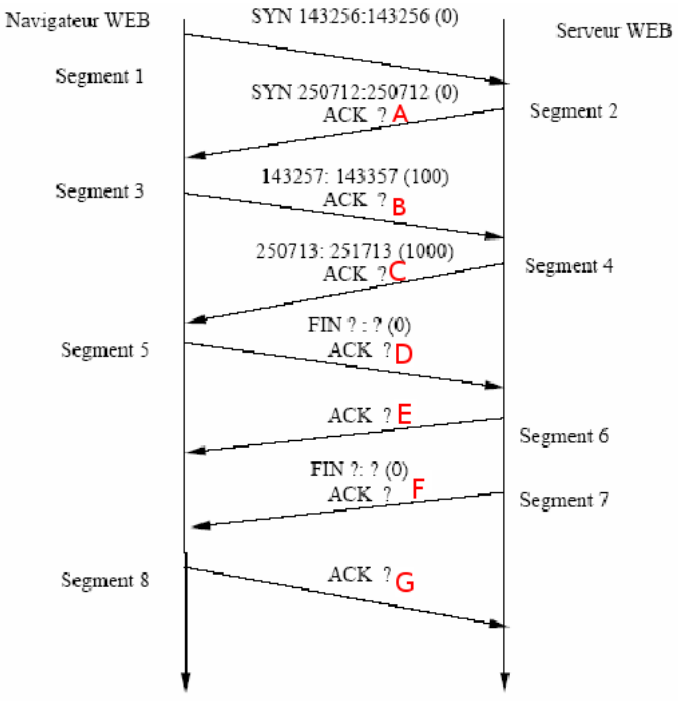


FIG. 25 – Donnée de la question 17

A : ACK 143257

B : ACK 250713

C : ACK 143358

D : FIN 143358 :143358 ; ACK 251714

E : ACK 143359

F : FIN 251714 :251714 ; ACK 143359

G : ACK 251715

8.18 Un accusé de réception perdu ne provoque pas nécessairement de retransmission. Expliquez pourquoi.

Dans TCP, les acquittements sont cumulatifs. Le prochain acquittement qui arrive peut confirmer aussi les données de l'acquittement perdu.

8.19 Expliquez pourquoi TCP ne permet pas de multicast ou de broadcast.

Le contrôle de flux nécessite une communication entre l'émetteur et le récepteur. L'émetteur s'adapte à la vitesse du récepteur. Dans une transmission multicast, l'émetteur devrait respecter la vitesse du récepteur le plus lent ce qui ne serait pas efficace.

8.20 On considère un réseau formé de deux routeurs. Sur le premier routeur se connecte un PC du client 1 et sur le second se connecte le PC du client 2. Les deux PC utilisent le logiciel TCP/IP pour leur connexion réseau.

a) Les routeurs doivent-ils posséder un logiciel TCP ?

b) En fait, le PC1 effectue principalement un transfert de fichiers FTP vers le PC2 sur le port 21. Les fragments émis ont une longueur de 8000 bits. Le premier segment émis possède le numéro de séquence 1. Quel est le numéro de séquence du deuxième segment émis ?

c) Supposons que les ACKs sont regroupés tous les quatres segments reçus. Quelle est la valeur portées dans le champ d'acquittement du premier paquet d'acquittement ?

a) Non, TCP opère sur les stations terminales, pas sur les routeurs.

b) TCP numérote les octets et non les segments. 8000 bits = 1000 octets donc le numéro de séquence du prochain segment sera 1001.

c) Si tout se passe bien (pas de perte de segment), le champ 'Numéro d'accusé de réception' contiendra la valeur 4001. (il attend l'octet qui a le numéro 4001).

8.21 Comment un Firewall peut-il interdire, pour des raisons de sécurité, l'accès à certaines applications d'une entreprise ?

Il suffit d'indiquer au firewall de bloquer le port (source, destination ou les deux) de l'application. Cette solution fonctionne pour autant que l'application ait un port bien connu.

8.22 Les flots qui utilisent le protocole UDP ne sont soumis à aucun contrôle de flux. Peuvent-ils devenir un problème pour les applications utilisant le protocole TCP ?

Oui, si un flot UDP occupe l'ensemble de la bande passante disponible alors le débit avec TCP, qui utilise des techniques de contrôle de congestion et de flux va être nul car le réseau sera tout le temps surchargé.

8.23 En quoi TCP n'est pas adapté au transfert de données qui ont des contraintes temps réel (contrainte de gigue constante, contrainte de latence bornée par exemple).

TCP n'est pas adapté au transfert de données ayant des contraintes temps réel car premièrement il effectue des retransmissions, et de plus TCP décide quand envoyer un paquet, qui n'est pas forcément quand l'application le demande.

8.24 Comment est programmé TCP pour qu'il n'y ait pas de confusion entre deux connexions successives, pour que les paquets de la première connexion qui a été interrompue de viennent pas interférer les paquets de la deuxième connexion ?

Pour éviter ce problème TCP permet de définir une valeur MSL (Maximum Segment Lifetime) afin de limiter la durée de vie d'un segment. La RFC de TCP préconise de ne pas réutiliser les mêmes sockets pour une nouvelle connexion avant l'écoulement de la $2 \cdot \text{MSL}$.

8.25 Expliquez la différence entre contrôle de flux et contrôle de congestion.

Le contrôle de flux adapte la vitesse de transmission à la vitesse du récepteur. Le récepteur contrôle la taille de la fenêtre glissante et peut ainsi varier la vitesse. Le contrôle de congestion adapte la vitesse de transmission à la capacité du réseau. L'émetteur adapte la taille de la fenêtre de congestion en utilisant les algorithmes de démarrage lent, évitement de congestion et l'accroissement additif et la décroissance multiplicative pour varier le seuil d'évitement de congestion en fonction des pertes de paquets.

8.26 Comment obtient-on un contrôle de flux dans TCP ?

En modifiant la taille de la fenêtre de l'émetteur, calculé grâce à un champ spécifique dans les acquittements du récepteur.

8.27 Qu'est-ce que le syndrome de la fenêtre stupide ? Expliquez dans quelle situation il peut se produire.

Le syndrome de la fenêtre stupide est un problème de performance de TCP dans lequel de très petits segments sont transmis bien que d'autres données attendent la transmission dans le tampon d'émission. Il peut se produire lorsque l'application au récepteur lit les

données octet par octet. Sans contre-mesures, TCP au récepteur annonce de petites tailles de fenêtre et l'émetteur n'a le droit que d'envoyer de petits segments.

8.28 Une machine TCP envoie des données avec une taille de fenêtre de congestion maximale sur un canal de 1Gb/s et un délai aller-retour de 2 ms. Quel est le débit maximum qu'on puisse atteindre ? Quelle est l'utilisation de la liaison ? Quelle est la taille de fenêtre nécessaire pour exploiter le lien à 100% ?

Les annonces de fenêtre du récepteur sont codées sur 16 bits. En conséquence, la taille maximale de la fenêtre glissante est de 65'535 octets. Selon la formule $U = \frac{W}{RTT \cdot C}$, l'utilisation maximum est donc $U = \frac{65535 \cdot 8 \text{ bits}}{0.02 \text{ s} \cdot 10^9 \text{ bits/s}} = 0.026$. Le débit maximum est donc de 26 Mb/s.

Pour une utilisation de 100%, il faudrait une taille de fenêtre de $W = RTT \cdot C = 0.02 \text{ s} \cdot 10^9 \text{ bit/s} = 2,5 \text{ Mo}$. Les nouvelles versions de TCP ont une option pour utiliser des fenêtres plus grandes que 64 Ko.

8.29 On considère un environnement dans lequel TCP opère sur un lien T3 (45 Mbit/s) et un temps de propagation aller-retour de 50 ms. Sachant que la taille des fenêtres de congestion est codée sur 16 bits, quelle est l'utilisation maximale du lien ?
Notez les résultats intermédiaires de votre calcul et calculez avec les unités (bits, secondes,. . .).

TCP peut transmettre le contenu d'un fenêtre par RTT, donc le débit maximum atteignable est de $D = \frac{65535 \text{ octets}}{50 \text{ ms}} = 1,3 \text{ Mo/s} = 10,5 \text{ Mb/s}$. L'utilisation maximum est donc limitée à $U = 10,5 \frac{\text{Mb/s}}{45 \text{ Mb/s}} = 0,233 = 23,3\%$.

8.30 Rappelez quels événements sont utilisés par TCP pour décider que le réseau est en congestion.

- Expiration d'un temporisateur d'envoi de paquet (aucun acquittement reçu) ;
- acquittements dupliqués reçus.

8.31 Expliquer brièvement l'objectif des algorithmes
a) démarrage lent
b) évitement de congestion
c) accroissement additif, décroissance multiplicative.

a) Démarrage lent : Le démarrage lent commence avec une fenêtre de congestion très petite (1 segment) mais l'augmente très rapidement. Il sert à atteindre rapidement un débit élevé au début d'une connexion ou après un timeout.

b) Évitement de congestion : L'évitement de congestion augmente la taille de la fenêtre de congestion lentement (1 segment par RTT) pour tester s'il est possible de transmettre plus rapidement. Il est utilisé dès que cwnd a dépassé le seuil d'évitement de congestion, donc dans une zone proche du débit optimal.

c) Accroissement additif, décroissance multiplicative : Cet algorithme varie la valeur du seuil d'évitement de congestion en fonction de la capacité du réseau et des pertes détectées. Lorsqu'il n'y a pas de congestion, le seuil ssthresh augmente lentement avec cwnd. C'est la phase d'accroissement additif. Lorsqu'une congestion est détectée due à une perte, ssthresh est diminué à la moitié et la valeur de cwnd est mise à ssthresh. Ainsi TCP diminue rapidement le débit de transmission. C'est la phase de décroissance multiplicative. Cet algorithme est nécessaire pour garantir la stabilité du réseau.

8.32 Quelle est la justification de la croissance exponentielle de la valeur du timeout proposé par Karn et Partridge ? Pourquoi est-ce qu'une croissance linéaire est moins bonne ?

Cela permet de diminuer la charge du réseau de manière exponentielle, si le réseau est vraiment surchargé.

8.33 Dans le diagramme de la figure 26, indiquez les mécanismes ('M :') de TCP (comme p.ex. 'démarrage lent') et les évènements ('E :') qui conduisent à l'évolution montrée de la fenêtre de congestion.
Choisissez parmi les mécanismes « Démarrage lent », « Évitement de congestion », « Retransmission rapide », « Évitement de la fenêtre stupide » et les évènements « Syndrome de la fenêtre stupide », « Trois acquittements dupliqués », « Timeout du temporisateur de retransmission ».

8.34 Sachant que TCP originalement mettait à jour son estimation du délai aller-retour (RTT : Round Trip Time) selon : SRTT $= \alpha \cdot SRTT + (1 - \alpha) \cdot RTT$**, où** RTT **est la dernière mesure obtenue et** $0 \leq \alpha < 1$**, quelles sont les conséquences d'une valeur de** α **proche à** 1 **et proche à** 0 **?**

Une valeur de α proche à 0 permet de s'adapter plus rapidement aux variations du RTT. Une valeur proche de α proche à 1 lisse d'avantage l'estimation et filtre les fluctuations rapides.

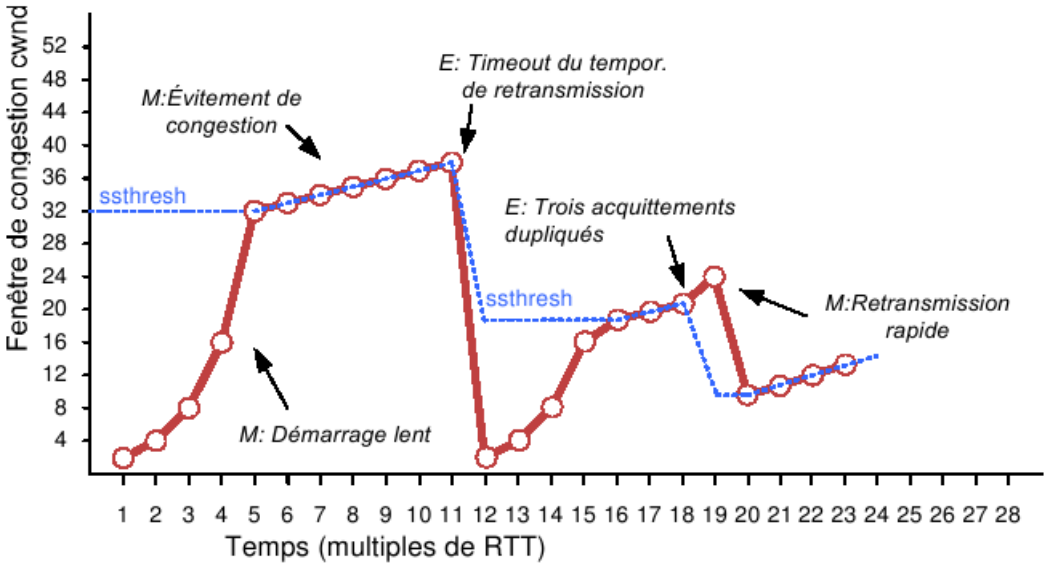


FIG. 26 – Donnée et réponse de la question 33

8.35 La méthode améliorée du calcul du RTT utilise les équations suivantes :
$Err = RTT - SRTT$
$SRTT = SRTT + g \cdot Err$
$D = D + h \cdot (|Err| - D)$
$RT_O = SRTT + 4 \cdot D$
avec $g = \frac{1}{8}$ **et** $h = \frac{1}{4}$**. Supposez que les estimations actuelles sont** $SRTT = 0,5$ **s et** $D = 0,2$ **s. Montrez l'évolution de** $SRTT$**,** D**, et** RT_0 **si les prochains 4 segments ont un délai aller retour mesuré de 1 s.**

	Estim.	*Seg 1*	*Seg 2*	*Seg 3*	*Seg 4*	*Seg 5*	*Seg 6*	*Seg 7*	*Seg 8*	*Seg 9*	*Seg 10*	*Seg 11*
RTT		1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Err		0.5	0.44	0.38	0.33	0.29	0.26	0.22	0.20	0.17	0.15	0.13
SRTT	0.5	0.56	0.62	0.67	0.71	0.74	0.78	0.8	0.83	0.85	0.87	0.88
D	0.2	0.28	0.32	0.33	0.33	0.32	0.31	0.29	0.26	0.24	0.22	0.2
RTO	1.3	1.66	1.88	1.99	2.04	2.04	2.0	1.95	1.88	1.81	1.74	1.67

On s'aperçoit que l'estimation du délai aller retour moyen, SRTT, augmente et s'approche à la nouvelle moyenne de 1s. L'estimation de l'écart, D, qui exprime les fluctuations des mesures, augmente au début, quand le RTT augmente brusquement. Après un certain nombre de mesures avec un RTT stable, D diminue et reflète ainsi que les mesures suivantes sont stables. La valeur de la temporisation de retransmission, RTO, augmente brusquement au début pour ensuite diminuer dès que les nouvelles mesures de RTT se stabilisent.

8.36 Quels sont les deux évènements qui provoquent la retransmission d'un segment TCP ? Autrement dit, comment un émetteur TCP détecte-t-il la perte d'un segment ?

L'expiration d'un temporisateur de retransmission (congestion sévère) et la réception de trois acquittements dupliqués (perte d'un ou plusieurs paquets, mais pas tous).

8.37 Pourquoi TCP attend-il 3 acquittements dupliqués avant de retransmettre un segment (retransmission rapide) ?

La réception de paquets en désordre déclenche également un acquittement dupliqué. Pour éviter de retransmettre un paquet qui n'a pas été perdu mais dépassé par un autre paquet, l'émetteur attend plusieurs acquittements dupliqués avant de déclencher une retransmission. Ainsi, il y a une probabilité élevée que le paquet ait vraiment été perdu.

8.38 Analyser le comportement de l'algorithme de démarrage lent sur une liaison sans congestion avec un temps aller retour de 10 ms. La fenêtre du récepteur fait 25 Ko et la taille maximum de segment 2 Ko. Combien de temps faut-il attendre avant de pouvoir envoyer la première fenêtre pleine ?

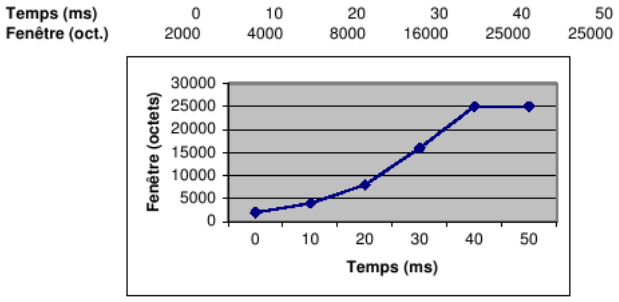


FIG. 27 – Réponse de l'exercice 38

Il faut 40 ms ou 4 RTT pour atteindre le débit maximum.

RTT	cwnd	ssthresh
0	65535	65535
1	1024	32767
2	2048	32767
3	4096	32767
4	8192	32767
5	16384	32767
6	32768	32768
7	33792	33792
8	34816	34816
9	35840	35840
10	36864	36864
11	37888	37888
12	38912	38912
13	39936	39936
14	1024	19968
15	2048	19968
16	4096	19968
17	8192	19968
18	16384	19968

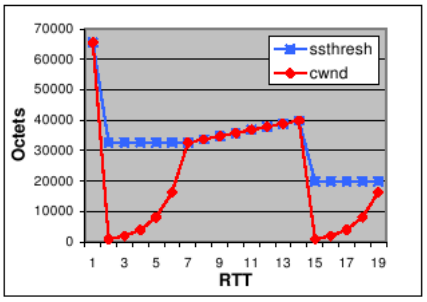


FIG. 28 – Réponse de l'exercice 39

8.39 **Tracer un diagramme illustrant l'évolution de la fenêtre de congestion (cwnd) de TCP en fonction du temps, sous les hypothèses suivantes :**
- la taille maximum de segment est de 1024 octets ;
- initialement, la fenêtre de congestion est de 64 Koctets ;
- l'unité de temps utilisée est le délai aller-retour (RTT) ;
- aux temps 0 et 14, le temporisateur de retransmission vient d'expirer.

8.40 **On considère un environnement dans lequel quatre stations (A, B, C et D) sont connectées sur un bus Ethernet. La courbe de l'image 29 présente le taux de transfert d'un fichier à l'aide du protocole FTP (utilisation de TCP) entre les stations A et B.**
Pourquoi le taux de transfert entre A et B devient nul lorsqu'un autre fichier est transféré entre les stations C et D (date t=40000) à l'aide du protocole TFTP (utilisation d'UDP) ?

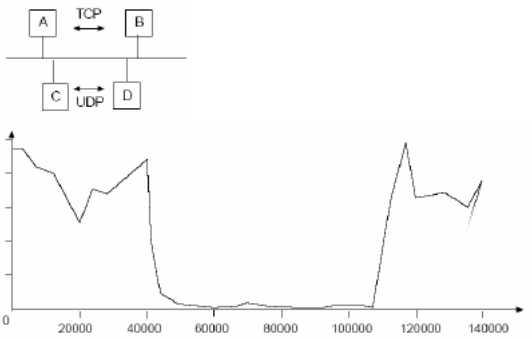


FIG. 29 – Réseau de l'exercice 40

UDP ne comporte ni de système de gestion de congestion ni de système de gestion de

flux. Par conséquent, UDP envoie les paquets à la vitesse maximum de l'interface de sortie de la machine. Comme le réseau est surchargé, TCP adapte son débit de manière à garder le réseau stable, c'est pourquoi son débit est aussi faible.

8.41 Expliquez pourquoi des timeouts « longs » sont encore possibles dans TCP même lorsque le mécanisme de retransmission rapide est utilisé.

La retransmission rapide (Fast Retransmit) est déclenchée par la réception de trois acquittements dupliqués. Mains le récepteur n'envoie des acquittements que quand il a reçu un paquet. Si plusieurs paquets de suite sont perdus, l'émetteur ne reçoit pas d'acquittements dupliqués et la retransmission est déclenchée par un timeout. Ceci se produit typiquement dans une congestion sévère, où beaucoup de paquets sont perdus.

8.42 Le protocole SMTP (Simple Mail Transfer Protocol) utilise TCP pour échanger du courrier électronique entre serveurs mail. Au début, les deux serveurs échangent plusieurs brefs messages pour s'identifier, négocier les options et indiquer le récepteur du courrier électronique à transmettre. Ensuite le fichier (qui peut être long) est transmis. Expliquez pourquoi ce comportement pose des problèmes pour le contrôle de congestion de TCP.

Pendant l'échange de messages brefs, la fenêtre de congestion s'ouvre avec le démarrage lent. Pendant cette phase, la transmission est très lente, similaire à un protocole requête-réponse. Il n'y a donc pas de risque de congestion. Après cette phase, le message est transmis. Puisque la fenêtre de congestion à été ouverte par le démarrage lent, toute une rafale de segments peut être envoyée au début de cette phase, ce qui peut facilement provoquer une congestion. Le problème est donc que l'application change brusquement de vitesse de transmission et le contrôle de congestion de TCP ne peut pas l'éviter.

8.43 Pourquoi pensez-vous que la probabilité d'élimination (drop probability) d'une passerelle RED n'augmente pas simplement linéairement depuis P=0 à MinThresh à P=1 à MaxThresh ?

Cette question n'a plus lieu d'être, le protocole RED ayant été modifié pour avoir une augmentation linéaire.