Licence et IUP GMI — Examen de Réseau — 2002-2003

(3 heures)

Les documents et calculatrices sont autorisés.
Ce sujet est composé de 5 parties indépendantes (1 partie par page). Chaque partie est notée sur 5 points.
***Il vous est demandé de choisir et de ne traiter que 4 parties sur les 5 proposées. Indiquez les numéros des 4 parties choisies en entête de votre copie**. Les réponses d'une éventuelle 5ème partie traitée sur votre copie ne seront pas corrigées.*

Partie I - Connexion physique

Un paquet IP est émis par une machine, ce paquet est d'abord transmis sur un réseau local, via une liaison Ethernet 100Mb/s (codage Manchester).
Le paquet IP est ensuite répété sur une liaison téléphonique via un modem 9600 Bauds, qui exploite :

- 2 niveaux de modulation d'amplitude pour coder le 1er bit (0 = 3V, 1 = 5V),
- 2 niveaux de modulation de fréquence pour coder le 2ème bit (0 =simple et 1=double),
- 2 niveaux de modulation de phase pour coder le 3ème bit (0=0° et 1=180°).

Enfin, il traverse l'océan atlantique via une fibre optique. Dans cette fibre, d'une longueur de 1500km, les signaux qui circulent à la vitesse de la lumière (300000km/s) sont transmis à raison de 4Gbits/s.

Question I.1

Sur le réseau local un oscilloscope mesure le signal suivant lors de l'émission du paquet :

Figure 1 : trame Ethernet

Décodez, sous la forme d'une série de nombres hexadécimaux, le début de ce morceau de trame Ethernet.

Question I.2

Si la trame Ethernet minimale n'est composée que de 40 octets, quelle est la longueur maximale du bus Ethernet, pour laquelle la carte réseau pourra détecter une collision (utilisation du protocole CSMA/CD) ?

N.B. Le signal électrique se propage dans le fil de cuivre à la vitesse de 200000 km/s.

Question I.3

Quel est le débit, en bit/s du modem ?
Le segment de données montré par la figure 1 est ensuite mesuré, après modulation. Quelle est la forme du signal que le modem transmet pour les 12 premiers bits que vous avez décodé en Question I.1 ?

Question I.4

Le paquet est ensuite démodulé et encodé en signaux lumineux pour être transporté sur la fibre optique. Combien de temps s'écoulera entre l'émission du premier bit sur la fibre optique en Europe et le décodage du dernier bit du premier octet en Amérique ? Sur combien de mètres le signal lumineux de cet octet s'étalera dans la fibre optique, lors de son voyage transatlantique ?

Partie II - Liaison de données

Nous considérons la table de codage de Hamming suivante pour 16 symboles :

Symbole	Code de Hamming	Symbole	Code de Hamming
(0) 0000	00000000000000	(1) 0001	00000001111111
(2) 0010	00011110000111	(3) 0011	00011111111000
(4) 0100	01100110011001	(5) 0101	01100111100110
(6) 0110	01111000011110	(7) 0111	01111001100001
(8) 1000	10101010101010	(9) 1001	10101011010101
(A) 1010	10110100101101	(B) 1011	10110101010010
(C) 1100	11001100110011	(D) 1101	11001101001100
(E) 1110	11010010110100	(F) 1111	11010011001011

Question II.1
Calculez la distance de Hamming minimale entre l'ensemble de symboles {0, 1, 2, 3}.

Question II.2
En considérant que la distance minimale que vous avez calculée (Min dH({0, 1, 2, 3})) est égale à la distance minimale de Hamming entre chaque symbole de la table (Min dH({0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F})), quelle est la capacité de « détection » de ce codage de Hamming et quelle est sa capacité de « correction » ?

Question II.3
Décodez le message suivant :
`11001100110011 10110100101111 11001101001111 00000000000111`

Question II.4
La procédure `getQuartet()` ci-dessous qui lit (et corrige éventuellement) un quartet encodé selon la table de symboles proposée précédemment. Cependant une erreur s'est glissée dans cette procédure, elle décode correctement les messages, mais ne corrige aucune erreur… (la procédure `dH()` qui calcule la distance de Hamming a déjà été vérifiée correcte). Il vous est demandé de corriger `getQuartet()`.

```
class decodeur
{
  final static int hcode[] = /* liste des codes de Hamming           */
  { 0x0000, 0x007F, 0x0787, 0x07F8, 0x1999, 0x19E6, 0x1E1E, 0x1E61,
    0x2AAA, 0x2AD5, 0x2D2D, 0x2D52, 0x3333, 0x334C, 0x34B4, 0x34CB} ;
  static int cValue = 0;   /* valeur lue sous forme 'encodée'         */
  static int nbOfBits = 0; /* nombre de bits valide dans cValue       */
  static int getQuartet(InputStream in) throws IOException {
    int hValue ;
    while(nbOfBits<14) {   /* lire (au moins) 14 bits dans in         */
      hValue= in.read();
      if(hValue == -1) return -1;       /* plus d'octets dans 'in' ? */
      cValue= cValue | (hValue<<nbOfBits) ;
      nbOfBits+=8;
    }
    hValue = cValue & 0x03FFF ;    /* hValue = 14 bits lus dans 'in' */
    cValue = cValue >> 14; nbOfBits -= 14;
    for(int i=0 ; i<15 ; i++)
      if(dH(hvalue,hcode[i])<1) return i; /* i : valeur décodée      */
    throw new IOException();
  }
  static int dH(int i,int j) {…} /* calcul de la distance de Hamming */
}
```

Partie III- Routage

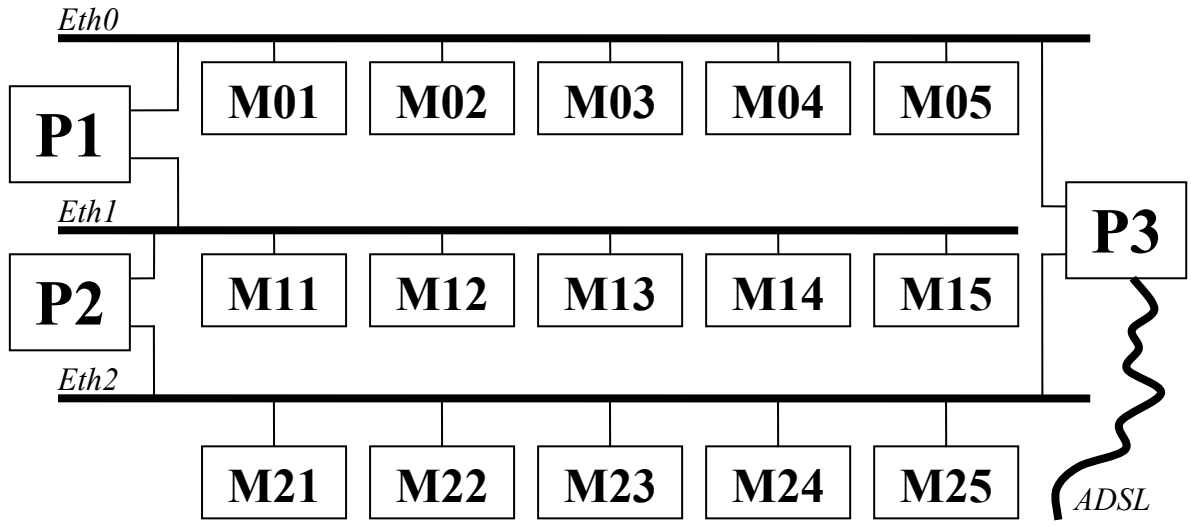

Figure 2 : Représentation d'un « réseau local »

Le réseau IPv4 (représenté ci-dessus) est composé de 3 bus Ethernet notés *Eth0*, *Eth1* et *Eth2* et de trois passerelles P1, P2 et P3. La passerelle P3, est connectée, via une liaison *ADSL* à Internet. Chaque bus supporte, en plus de deux passerelles, 5 machines. Ces machines utilisent des adresses IPv4 **Intranet** de classe **B**.

Question III.1
Proposez un masque de sous réseau commun global pour identifier les réseaux associés à *Eth0*, *Eth1* et *Eth2*. Proposez une adresse de sous réseau pour chaque bus Ethernet et finalement, une adresse IP pour chaque machine du réseau, (2 adresses IP pour les machines passerelles P1, P2 et P3).

Question III.2
Donnez les tables de routages pour les passerelles P1, P2 et P3. Chaque table contiendra 4 champs : adresse Réseau, masque réseau, adresse Passerelle, Liaison.
N.B. Il est inutile de définir la liaison si la passerelle est définie, et dans le cas par « défaut » inutile de préciser adresse de réseau et masque…

Question III.3
L'utilisateur de la machine M25 a défini sa table de routage IP comme suit :

```
$route –n
default P3
```

Pourquoi cette configuration permet effectivement à sa machine d'utiliser le réseau local ? Mais pourquoi est-elle sous optimale ? Quelle est la table de routage optimale pour cette machine ? Deux passerelles auraient suffit pour rendre le réseau exploitable, en quoi la présence de la troisième passerelle permet d'optimiser le fonctionnement global du réseau ?

Question III.4
La passerelle P3 est connectée à Internet via une liaison ADSL. Comment configurer la table de routage de P3 pour qu'elle route les paquets IP vers/depuis Internet ? Pourquoi malgré cela, les machines du réseau, telles qu'elles sont définies actuellement, ne peuvent pas communiquer avec des machines présentes sur Internet ?

Partie IV - Transport

Nous nous intéressons ici au fonctionnement d'un jeu vidéo en réseau. Le fonctionnement de ce jeu repose sur deux programmes distincts :

- le moteur du jeu (noté CJ), qui gère l'interface avec l'utilisateur, ce programme s'exécute sur chaque ordinateur client ;
- le serveur (noté SJ), qui recoupe les actions de l'ensemble des joueurs pour déterminer l'évolution globale du jeu. Ce programme s'exécute sur un serveur central géré par la maison de jeu.

Le serveur SJ accepte un nombre moyen de 5000 connexions simultanées, via des socket TCP clientes provenant des CJs. Cependant, pour que le jeu fonctionne correctement il faut que le temps de transmission d'une structure d'informations élémentaire (contenu dans un paquet IP) entre chaque CJ et le SJ, ne dépasse pas 100ms (dans le cas contraire le client est refusé). Des mesures expérimentales ont montré que le client transmet un volume moyen de données de 2Ko/s. Il s'agit en fait de données relatives aux actions du joueur. En réponse le serveur renvoie un volume de 20Ko/s. Ce sont des données relatives à l'environnement virtuel du joueur, fonction de ses actions et des actions des autres joueurs, à un instant donné.

Question IV.1
Initialement le système d'exploitation installé sur le serveur réserve 64Ko de mémoire pour le tampon d'émission et 64Ko pour le tampon de réception de chaque Socket. Combien de mémoire centrale le serveur SJ est-il amené à réserver pour les tampons de l'ensemble des sockets TCP en moyenne ? Pendant combien de secondes le serveur SJ peut continuer à transmettre des données sans recevoir d'ACK des CJs (et sans être obligé de re-émettre des données) ?

Question IV.2
Il est dit dans l'énoncé que les délais des messages échangés entre SJ et les CJs n'excèdent pas 100ms. En supposant qu'il n'y ait pas d'erreur de transmission et que les programmes CJs consomment les données dès leur réception, quel est le délais minimum pendant lequel les données reçues vont devoir rester dans le tampon du serveur (avant qu'il n'ait reçu d'ACK du client) ? Quelle est alors la taille minimale du tampon d'émission du serveur SJ ?

Question IV.3
Quelle est la taille minimale du tampon de réception dans les mêmes conditions ? En considérant maintenant que les tampons d'émission et de réception du serveur sont reconfigurés avec les valeurs que vous avez calculées quelle est la taille totale des tampons TCP du serveur en moyenne (5000 connexions TCP) ?

Question IV.4
Les informations transmisses par le SJ aux CJs sont « temps réel », c'est-à-dire que les programmes CJ n'ont pas besoin de toutes les données transmises par le SJ mais seulement des données les plus « fraîches » (les plus récentes). Pour alléger encore la charge réseau du serveur les programmeurs du jeu se proposent d'utiliser le protocole UDP plutôt que TCP. Comment justifiez-vous leurs choix ? En considérant que les Paquets UDP peuvent arriver dans un ordre différent de celui dans lequel ils ont été émis, proposez, en quelques lignes, une stratégie simple pour permettre au client CJ d'ignorer les paquets « en retard ».

Partie V - Serveurs FTP et HTTP

Des pirates ont détourné le fonctionnement normal d'un serveur FTP « public » nommé `ftp.dompub.fr` (IP : `103.49.225.11`) pour que cette machine contribue à l'attaque d'un serveur HTTP (web) nommé `www.security.com` (IP: `66.37.222.8`). Après analyse des « fichiers de log » du serveur FTP, il apparaît que les pirates se sont connectés sur le serveur FTP, qu'ils ont transféré un fichier (nommé `GET.CMD` au format texte) sur ce serveur, puis qu'ils ont demandé le transfert de ce fichier depuis le serveur FTP un grand nombre de fois… La plainte est venue des administrateurs du serveur HTTP qui ont la preuve que c'est le serveur FTP qui c'est connecté un grand nombre de fois sur leur site et a ainsi rendu le serveur HTTP inexploitable pendant plus d'une heure.

Contenu (abrégé) du fichier `GET.CMD` :

```
GET ////////////////////////////// HTTP/1.0 <EOL>
Accept: */* <EOL>
Accept-Language: fr <EOL>
User-Agent: Mozilla/4.0 <EOL>
Host: www.google.fr <EOL>
Proxy-Connection: Keep-Alive <EOL>
<EOL>
<EOF>
```

(Dans le fichier réel il y a 1024 '`/`' dans la première ligne).

Question V.1
Les administrateurs de la machine `www.security.com` « attaquée » pensent que c'est le « service FTP » de la machine `ftp.dompub.fr` qui a été détourné de son fonctionnement normal pour réaliser « l'attaque ». En supposant que le serveur Web garde une trace de chaque connexion cliente en enregistrant notamment {AdresseSource, PortSource, AdresseDestination, PortDestination} Comment les administrateurs peuvent désigner le service FTP (plutôt que n'importe quel autre service installé sur le serveur FTP) comme étant **LE** responsable du problème ?

Question V.2
Donnez la séquence des commandes du protocole FTP que les pirates ont transmis au serveur FTP, via le canal de contrôle, pour demander le transfert du fichier `GET.CMD` depuis leur machine cliente jusqu'au serveur (le serveur ftp « public » accepte les connexions anonymes).

Question V.3
Il est possible de configurer le service FTP de la machine `ftp.dompub.fr` en indiquant une liste d'opérations du protocole FTP que le serveur ne doit pas accepter. Un administrateur du serveur ftp pense qu'il suffit d'interdire la commande ftp `PASV` pour qu'on ne puisse plus détourner le fonctionnement du serveur FTP, un autre pense au contraire que c'est en interdisant la commande `PORT` que les hackers ne pourront plus détourner l'usage du serveur FTP. Lequel a raison ? Pourquoi ?

Question V.4
Donnez la série de commande FTP que les pirates ont transmis pour que le serveur `ftp.dompub.fr` « attaque » le serveur HTTP `www.security.com` (ainsi que les réponses plausibles du serveur FTP) ?