

# Exercices dirigés

Unité d'enseignement NFP 104

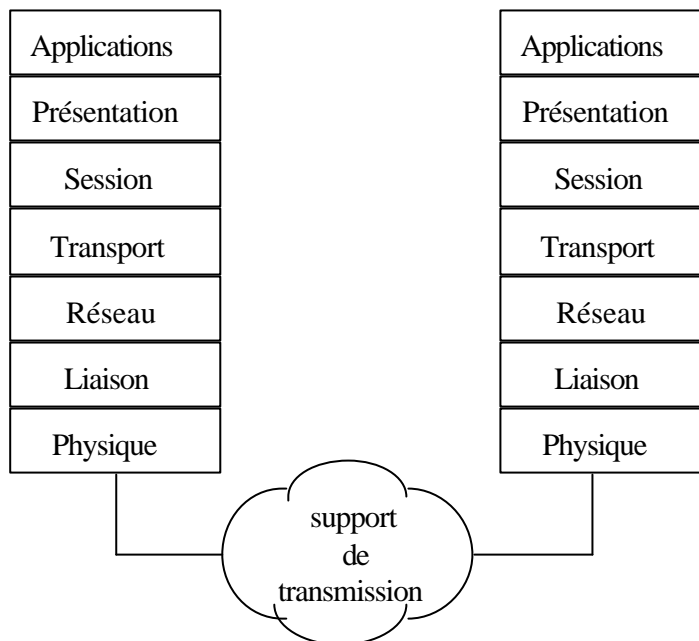
## Réseaux et protocoles

2007-2008

*Ce polycopié a été élaboré par l'équipe enseignante "Réseaux et protocoles" à partir d'exercices rédigés par MM. Berthelin, Cubaud, Farinone, Florin, Gressier-Soudan et Natkin.*

# 1• Les couches de protocoles

## Exercice 1 : Le modèle OSI



*Dans le contexte du modèle OSI, qu'est qu'une PDU ?*

*Quel est le nom donné aux unités de transfert pour les différentes couches ?*

*Qu'est qu'une primitive de service ?*

*Qu'est qu'une machine protocolaire ?*

*Donnez quelques exemples de piles protocolaires.*

## Exercice 2 : La couche physique

Vous devez construire une architecture de réseau local dans une salle informatique contenant 15 postes de travail. Le réseau local choisi est un Ethernet à 10 Mbit/s. Vous avez a votre disposition un extrait d'une documentation technique :

<i>normes</i>	<i>connecteurs</i>	<i>câbles</i>	<i>longueur max</i>	<i>topologie</i>	<i>coupleur réseau</i>
<b>10Base T</b>	RJ45	paire torsadée/UTP5	100m	Étoile	carte TX
<b>10Base 2</b>	BNC	coaxial fin	185m	Bus	carte BNC
<b>10Base 5</b>	Prise vampire	coaxial épais	500m	Bus	carte AUI

*Quel type de câblage préconiserez vous ?*

*Calculez le nombre de segments de cables nécessaires.*

## Exercice 3 : La couche Liaison

### Question 1. La trame Ethernet

Le format de l'information qui passe sur le médium de communication est le suivant, ce qui est en gras matérialise la trame Ethernet :

Préambule	Délimiteur de début	Adresse destination	Adresse source	Type	Informations	FCS
7 octets	1 octet	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

*Quelle est la longueur d'une trame minimum ?*

*Quelle est la longueur minimum de données transportables ?*

*Pourquoi la couche physique ajoute un préambule ?*

Voici la trace hexadécimale d'une communication point à point prélevée par un espion de ligne (SNOOP):

```
00: 0800 2018 ba40 aa00 0400 1fc8 0800 4500    .. ..@.....E.
16: 0028 e903 4000 3f06 6a5c a3ad 2041 a3ad    .(..@.?.j\.. A..
32: 80d4 0558 0017 088d dee0 ba77 8925 5010    ...X.....w.%P.
48: 7d78 1972 0000 0000 0000 0000 0000 0000    }x.r.....
```

*Retrouver les champs de la trame Ethernet dans la trace hexadécimale précédente.*

### Question 2. Adressage (adresse MAC)

Voici un exemple d'adresse Ethernet (6 octets) : 08:0:20:18:ba:40

*Deux machines peuvent-elles posséder la même adresse ethernet ? Pourquoi ?*

Voici la trace d'une communication point à point prélevée par un espion de ligne (SNOOP) :

```
ETHER: ----- Ether Header -----
ETHER: Packet 1 arrived at 18:29:10.10
ETHER: Packet size = 64 bytes
ETHER: Destination = 8:0:20:18:ba:40, Sun
ETHER: Source      = aa:0:4:0:1f:c8, DEC (DECNET)
ETHER: Ethertype  = 0800 (IP)
```

à comparer avec une communication à un groupe:

```
ETHER: ----- Ether Header -----
ETHER: Packet 1 arrived at 11:40:57.78
ETHER: Packet size = 60 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:18:ba:40, Sun
ETHER: Ethertype  = 0806 (ARP)
```

*Quel champ, par sa valeur permet de différencier les deux types de traces pour les communications à un seul destinataire ou à plusieurs destinataires ?*

*Comment un seul message peut-il parvenir à plusieurs destinataires simultanément ?*

## Exercice 4 : La couche Réseau

### Question 1. Adressage IPv4

Une adresse IPv4 est définie sur 4 octets. L'adressage IPv4 (Internet) est hiérarchique. Un réseau IPv4 est identifié par son numéro de réseau. Une machine est identifiée par son numéro dans le réseau. L'adresse IPv4 d'une machine est donc composée d'un numéro de réseau et d'un numéro de machine.

Exemple pour le CNAM (autrefois), la machine 'asimov' avait l'adresse IPv4 192.33.159.6 avec 192.33.159 (3 octets : réseau) et .6 (1 octet : la machine 'asimov' dans le réseau 192.33.159).

*Sur l'internet, deux machines à deux endroits différents peuvent elles posséder la même adresse IPv4 ?, si oui, à quelle condition ?*

*Dans le même réseau IPv4, deux machines différentes peuvent elles posséder la même adresse IPv4 à deux moments différents ? Chercher un contexte d'utilisation.*

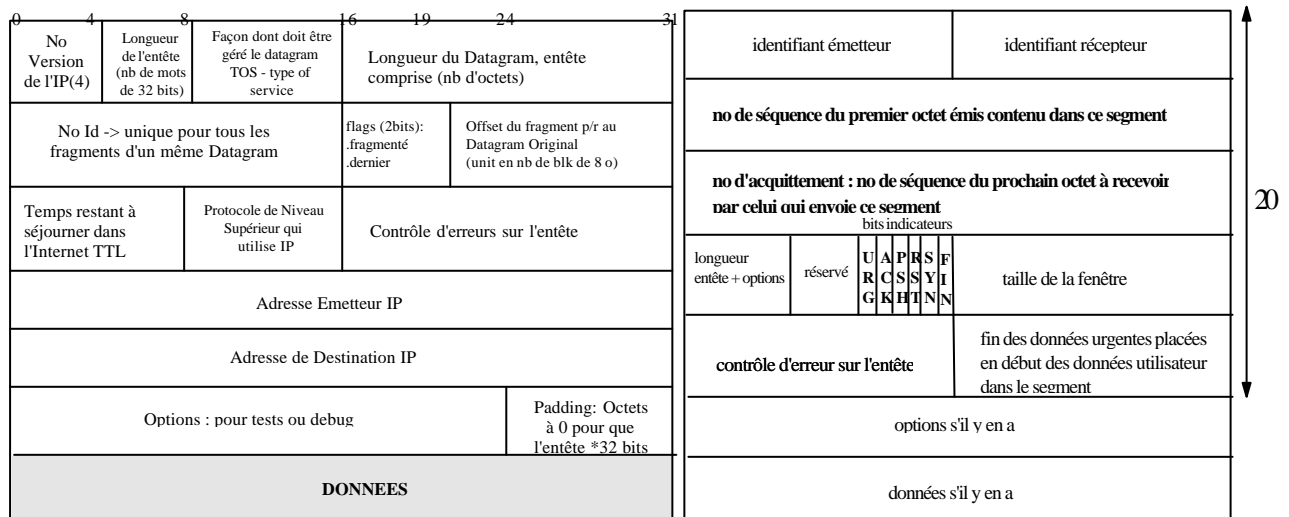
Voici l'affichage de la commande UNIX 'ifconfig' sur une machine :

```
le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
    inet 192.33.159.212 netmask ffffffff broadcast 192.33.159.255
    ether 8:0:20:18:ba:40
```

*A votre avis que montre cette commande ?*

## Exercice 5 : La couche Transport

On donne la structure de l'entête IP et la structure de l'entête TCP :



Trace d'une communication point à point prélevée par SNOOP :

```
ETHER: ----- Ether Header -----
ETHER: Packet 3 arrived at 11:42:27.64
ETHER: Packet size = 64 bytes
ETHER: Destination = 8:0:20:18:ba:40, Sun
ETHER: Source      = aa:0:4:0:1f:c8, DEC (DECNET)
ETHER: Ethertype = 0800 (IP)
IP: ----- IP Header -----
IP: Version = 4
IP: Header length = 20 bytes
IP: Type of service = 0x00
IP:   x xx. .... = 0 (precedence)
IP:   ...0 .... = normal delay
IP:   .... 0... = normal throughput
IP:   .... .0.. = normal reliability
IP: Total length = 40 bytes
IP: Identification = 41980
IP: Flags = 0x4
IP:   .1.. .... = do not fragment
IP:   ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 63 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = af63
IP: Source address = 163.173.32.65, papillon.cnam.fr
IP: Destination address = 163.173.128.212, jordan
IP: No options
TCP: ----- TCP Header -----
TCP: Source port = 1368
TCP: Destination port = 23 (TELNET)
TCP: Sequence number = 143515262
TCP: Acknowledgement number = 3128387273
TCP: Data offset = 20 bytes
TCP: Flags = 0x10
TCP:   ..0. .... = No urgent pointer
TCP:   ...1 .... = Acknowledgement
TCP:   .... 0... = No push
TCP:   .... .0.. = No reset
TCP:   .... ..0. = No Syn
TCP:   .... ...0 = No Fin
TCP: Window = 32120
TCP: Checksum = 0x3c30
TCP: Urgent pointer = 0
TCP: No options
TELNET: ----- TELNET: -----
TELNET: ""
```

*A votre avis, à quoi correspondent les étiquettes TCP et TELNET ?*

*Combien y a-t-il d'encapsulations successives ?*

Trace hexadécimale d'une communication point à point :

```
3  0.00000 papillon.cnam.fr -> jordan      TELNET C port=1368
00: 0800 2018 ba40 aa00 0400 1fc8 0800 4500  .. ..@.....E.
16: 0028 a3fc 4000 3f06 af63 a3ad 2041 a3ad  .(.ü@.?..c.. A..
32: 80d4 0558 0017 088d de7e ba77 66c9 5010  ...X.....~.wf.P.
48: 7d78 3c30 0000 0000 0000 0000 0000 0000  }x<0.....
```

*Déterminer le début du paquet IPv4.*

*Déterminer la fin de l'entête du paquet IPv4.*

*Déterminer la fin de l'entête TCP.*

# 2• Couche Physique

## Exercice 1 : Shanon et Nyquist

Un support physique de communication a une bande passante de 1 MHz.

### Question 1

*Quel est le débit maximum théorique d'information pouvant circuler sur ce support lorsqu'on utilise une modulation de valence 2 (bivalente) ?*

### Question 2

Le signal généré dans cette voie est tel que le rapport signal à bruit obtenu est de 20 dB.

*Quel est le débit maximum théorique d'informations pouvant être acheminées par cette voie ?*

*Quelle valence faudrait-il pour approcher ce débit maximum théorique ?*

## Exercice 2 : Théorème de Shannon

On rappelle que le modem V29 fonctionne à 9600 bit/s sur liaison 4 fils en full duplex. Le procédé de modulation est une modulation combinée de phase octovalente et de modulation d'amplitude bivalente (pour chaque phase utilisée on code en amplitude deux niveaux). On suppose que l'on utilise une voie physique de largeur de bande 3200 Hz.

### Question 1

*Quelle est la valence du signal modulé ? Quelle est sa rapidité de modulation ?*

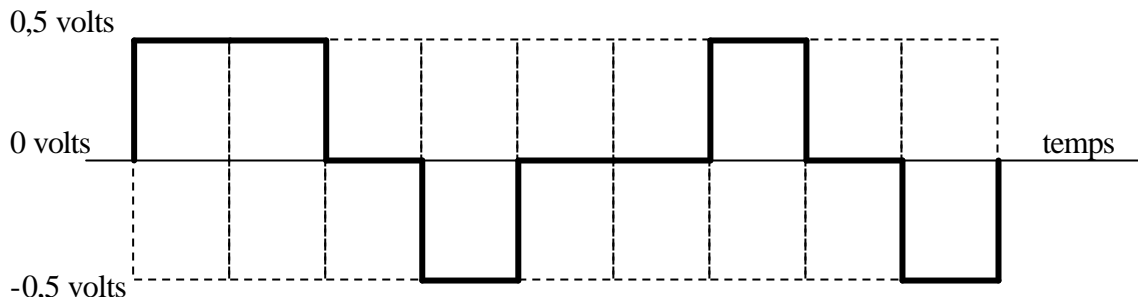
### Question 2

*Quel est le rapport signal à bruit minimum permettant la transmission, si l'on suppose que la voie est soumise à un bruit blanc gaussien (formule de Shanon) ?*

*Si le rapport signal à bruit est de 10 dB, la transmission est-elle possible ?*

## Exercice 3 : Modulations

Vous apercevez sur un oscilloscope branché sur un câble de réseau local un signal (tracé en trait gras). Ce signal correspond au codage (à la modulation) des bits au niveau physique dans un réseau local très répandu.



### Question 1

*Ce signal est-il celui d'un codage en bande de base ou celui d'un codage en modulation d'onde porteuse (justifiez votre réponse)?*

### Question 2

*Quel est le nom de ce codage de signal (expliquez pourquoi vous choisissez ce codage parmi tous les codages vus en cours à propos des réseaux locaux) ?*

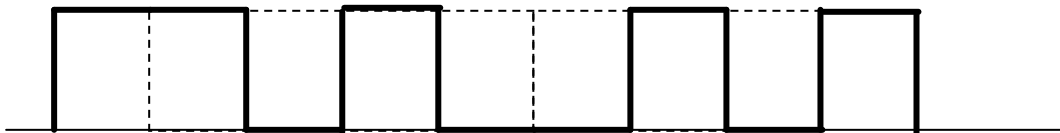
### Question 3

*Quelle est la suite binaire codée par ce signal ?*

### Question 4

*Quel est le nom du réseau local qui est testé (définition précise du type, du débit et du médium utilisé).*

Vous observez maintenant le signal suivant, toujours sur un réseau local répandu.



### Question 5

*Quel est le nom du codage utilisé dans ce réseau local est quel est le nom du réseau local (définition précise du type, du débit et du médium utilisé).*

### Question 6

*Quelle est la suite binaire transmise par le signal précédent ?*



## Exercice 4 : Utilité de la détection d'erreurs

Sur une liaison hertzienne urbaine à 1200 bit/s, on envoie des messages de 64 bits. La fréquence d'émission est de 12 messages/seconde.

### Question 1

*Calculer le taux d'utilisation de la liaison.*

La liaison étant de mauvaise qualité, le taux d'erreur par bit (noté  $p$ ) est compris entre 0,01 et 0,001.  $p$  représente la probabilité qu'un bit soit mal reçu.

### Question 2

*Calculer en fonction de  $p$  la probabilité qu'un message soit mal reçu. On suppose que les altérations des bits sont indépendantes.*

On suppose que l'émetteur sait quand un message est mal reçu et qu'il le retransmet.

### Question 3

*Calculer en fonction de  $p$  le nombre moyen de transmissions. Est-il possible de respecter (en négligeant le temps écoulé entre 2 retransmissions) la fréquence d'émission de 12 messages/seconde ?*

## Exercice 5 : Codes de contrôle d'erreurs à parités

Lorsque l'on ajoute un bit de parité à un caractère 7 bits pour en faire un caractère 8 bits on ajoute un contrôle d'erreur qui est dit à parité verticale (en anglais VRC pour 'Vertical Redundancy Check'). On parle aussi parfois de parité transversale.

### Question 1

*Rappelez la définition de la parité.*

### Question 2

*Pour caractériser les codes de contrôle d'erreur on utilise la distance de Hamming. Rappelez la définition de la distance de Hamming? Qu'est ce que la distance d'un code?*

### Question 3

*Pour des caractères 7 bits, le fait d'ajouter une parité verticale à chaque caractère, permet de définir le code de contrôle d'erreurs à parité verticale. Quelle est la distance de ce code?*

Indications : Pour déterminer cette distance vous considérerez une information de base à transmettre qui est ici un caractère sans sa parité (par exemple le caractère B en ASCII 7 bits 1000001). Vous prendrez un caractère voisin obtenu en modifiant un seul bit parmi les 7 bits du caractère. Vous en déduirez par le nombre de bits modifiés dans le mot du code à parité (à 8 bits) une indication sur la distance de ce code. Si possible vous chercherez à démontrer que la distance proposée est bien la bonne dans tous les cas.

#### Question 4

*On considère un code quelconque ayant comme propriété que sa distance est  $D$ . Combien d'erreurs ce code permet-il de détecter ? Combien d'erreurs permet-il de corriger ? Application numérique aux propriétés de détection d'erreurs et de corrections d'erreurs du code à parité verticale dont vous avez déterminé la distance à la question précédente.*

Pour une suite de caractères ASCII avec parité verticale on ajoute souvent, pour renforcer la qualité d'un code basé sur le contrôle de parité, un octet supplémentaire dont chaque bit est la parité de la chaîne de bits dans le message de même position. On parle alors de parité longitudinale (en anglais LRC pour Longitudinal Redundancy Check). Par exemple pour la suite de caractères 'BONJOUR!' les parités verticales et longitudinales sont notées respectivement dans l'exemple qui suit par des bits  $x$  et  $y$ . La parité longitudinale des parités verticales est notée  $z$ . On l'appelle quelquefois la parité croisée. C'est aussi la parité verticale des parités longitudinales.

	B	O	N	J	O	U	R	!	LRC
	1	1	1	1	1	1	1	0	$y=1$
	0	0	0	0	0	0	0	1	$y=1$
	0	0	0	0	0	1	1	0	$y=0$
	0	1	1	1	1	0	0	0	$y=0$
	0	1	1	0	1	1	0	0	$y=0$
	0	1	1	1	1	0	1	0	$y=1$
	1	1	0	0	1	1	0	1	$y=1$
VRC	$x=0$	$x=1$	$x=0$	$x=1$	$x=1$	$x=0$	$x=1$	$x=0$	$z=0$

Le fait d'ajouter les deux parités à une suite de caractères 7 bits (une parité verticale et une parité longitudinale) permet de définir un autre code de contrôle d'erreurs sur le message constitué d'une suite de caractères 7 bits.

#### Question 5

*Quelle est la distance de ce code ?*

Indication : pour déterminer cette distance vous considérerez l'un des caractères avec sa parité (comme le caractère B en ASCII). Vous modifierez un seul bit parmi les 7 bits du caractère et vous en déduirez par le nombre de bits modifiés dans tout le message (sur les parités) ce qui vous donnera une hypothèse sur la distance du code. Vous chercherez à montrer dans tous les cas que cette distance est la bonne.

#### Question 6

*Pour un code avec parité verticale et longitudinale, combien d'erreurs peuvent être détectées, combien d'erreurs peuvent être corrigées?*

#### Question 7

*Pour un code avec parité verticale et longitudinale expliquez concrètement comment les résultats de la question précédente s'interprètent.*

Indications : comment peut-on détecter le nombre d'erreurs que vous avez indiqué et corriger le nombre d'erreurs que vous avez indiqué.

## Exercice 6 : Codes polynômiaux

On considère le code polynomial sur 14 bits généré par le polynôme  $G(x)=x^4 + x + 1$

### Question 1

Rappeler le principe des codes polynômiaux. Quel est le nombre de bits de redondance qui seront ajoutés par  $G$  ? Quelle est la taille des mots initiaux ? Ce code permet de détecter quels types d'erreurs ?

On veut calculer les bits de redondance du mot  $M=1101011011$

### Question 2

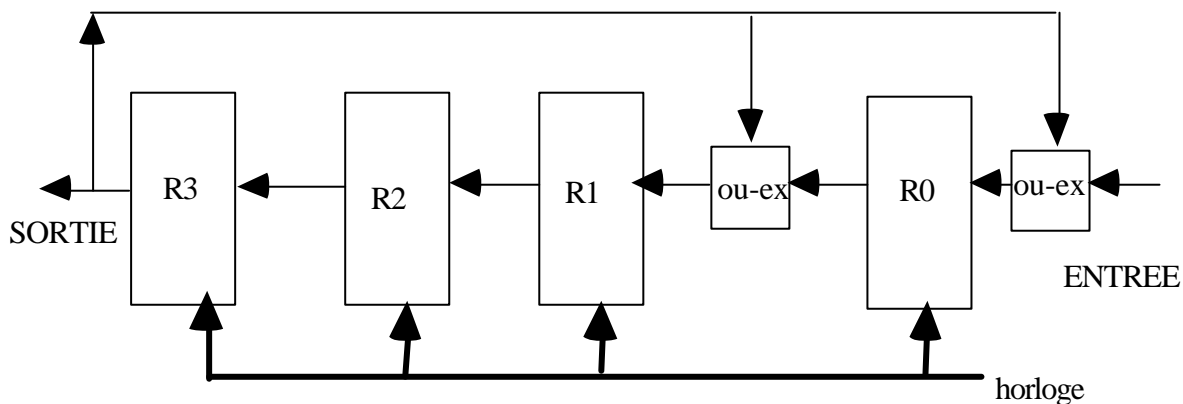
Donner  $D(x)$ , le polynôme correspondant à  $M$ .

### Question 3

Calculer  $R(x)$ , le reste de la division euclidienne de  $D(x).x^4$  par  $G(x)$ . En déduire la valeur des bits de redondance.

Les bits de redondances sont en général fabriqués par un dispositif matériel assez simple, utilisant des portes logiques et des registres à décalage.

Pour cet exemple, le circuit a le schéma suivant :



Le circuit reçoit en entrée les bits du mot  $M$  (le bit de poids fort d'abord). Les registres  $R0 \dots R3$  sont initialisés à zéro. Au 4<sup>ème</sup> coup d'horloge, ils ont tous reçu une valeur. Au 10<sup>ème</sup> coup, tous les bits de  $M$  ont été chargés. C'est pendant les 4 coups suivants que se fabriquent les bits de redondance.

### Question 4

Donner le contenu des registres pour chaque coup d'horloge.

## Exercice 7 : Code correcteur d'erreur linéaire

On suppose qu'un code pour coder des messages de trois bits est construit en utilisant les mots de codes de six bits, c'est-à-dire qu'aux trois bits de données à transmettre, on ajoute trois bits de redondance pour former des messages transmis de 6 bits :

Message à transmettre	Message transmis
000	000000
100	100110
010	010011
110	110101
001	001101
101	101011
011	011110
111	111000

### Question 1

*Un destinataire reçoit le message 101111. Est ce un message correct ?*

### Question 2

*Un destinataire reçoit le message 101111. En utilisant ce code comme un code correcteur d'erreurs, par quel message doit il être corrigé (quel est le message transmis) ?*

### Question 3

*Le code étudié dans ce problème est un code linéaire. Dans un code linéaire la distance du code est égale au plus faible poids d'un message correct (ou encore à la distance qui sépare le message 0000...000 du message le plus proche). Quelle est la distance du code défini dans ce texte ?*

### Question 4

*De combien d'erreurs un code de distance  $D$  est-il détecteur ? De combien d'erreurs ce code est-il correcteur ?*

### Question 5

*A partir des mots du code comment peut-on construire la matrice  $G$  (la matrice génératrice du code) ? Montrez que la matrice génératrice de ce code linéaire est la matrice  $G$  suivante ?*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

### Question 6

*Quelle est la matrice de contrôle de ce code linéaire ? Montrez au moyen de la matrice de contrôle que le message 100110 est correct et que le message 101111 est incorrect.*

# 3• Niveau liaison (1)

## Exercices généraux

### Exercice 1 : Délimitation des trames

On doit émettre les données binaires suivantes (4 octets) :  
0011 0111 0111 1110 0001 0001 1011 1110 soit encore en hexadécimal 377E11BE

#### Question 1

*La délimitation des trames utilisée dans les protocoles type HDLC est la transparence binaire ("bit stuffing"). Rappelez brièvement son principe.*

#### Question 2

*Quelle trame observerait-t-on sur une voie physique si la délimitation HDLC et la procédure de transparence binaire sont utilisées pour la suite binaire précédente ?*

#### Question 3

*Pour des trames comportant un nombre entier de caractères 8 bits la délimitation par transparence caractère "character stuffing" peut-être aussi utilisée. Rappelez brièvement son principe.*

#### Question 4

*Le protocole PPP utilise la transparence caractère dans son fonctionnement de base ('PPP in HDLC framing'). Quelle suite de bits observe-t-on sur la voie physique pour la transmission en PPP de la suite binaire si la table des caractères soumis à la transparence (table ACCM 'Asynchronous Control Character Map') a défini en dehors du fanion tous ceux qui sont inférieurs à 32 (en décimal). Donnez le résultat en hexadécimal ?*

### Exercice 2 : Bienfaits de l'anticipation

Pour transmettre des messages entre deux stations A et B, on utilise un satellite situé à 36000 km de la terre. Les messages font 1000 bits et le débit de la liaison est de 50 Kb/s. On rappelle que le délai de propagation d'une onde électromagnétique dans l'espace est voisin de la vitesse de la lumière, soit 300000 km/s.

*Quel est le temps de transmission d'un message de A vers B ?*

On utilise une procédure dite d'attente réponse : A envoie un message vers B et attend que B acquitte ce message pour en envoyer un autre. Le message d'acquiescement fait 100 bits.

*Calculer le débit effectif de la liaison et son taux d'utilisation.*

Au vu des résultats précédents, on décide de faire de l'anticipation, c'est à dire que A peut envoyer K messages au maximum avant de recevoir l'acquiescement du premier (il y a un message d'acquiescement par message émis).

*Calculer la valeur de  $K$  qui maximise le taux d'utilisation.*

### **Exercice 3 : Gestion des fenêtres**

On désire programmer un protocole dont les qualités sont les suivantes :

- bidirectionnel,
- avec anticipation ,
- acquit positif porté par les trames,
- et tel que le récepteur n'accepte les messages qu'en séquence.

#### **Question 1**

*A quelles conditions d'erreurs sur la liaison de données les spécifications précédentes correspondent-elles ?*

#### **Question 2**

*Montrer plusieurs situations d'utilisation de l'acquittement dans un échange d'information bidirectionnel.*

*Rappeler le principe du piggybacking.*

#### **Question 3**

*A quoi sert le mécanisme de temporisation ?*

#### **Question 4**

*Rappeler le principe du contrôle de flux dans la liaison de données. A quoi sert-il ?*

#### **Question 5**

*Rappeler brièvement pour les protocoles de liaison le principe de la gestion des fenêtres en émission*

On suppose que chaque émetteur peut utiliser au maximum  $\text{Maxseq}+1$  numéros de séquence différents numérotés de 0 à  $\text{Maxseq}$  (numérotation en modulo  $\text{Maxseq}+1$ ).

*Expliquer pourquoi la taille de la fenêtre en émission doit rester inférieure à  $\text{Maxseq}$  quand la taille de la fenêtre en réception vaut 1.*

*Mettre en évidence un cas d'ambiguïté.*

#### **Question 6**

*Quelle est la taille de la fenêtre en réception pour le protocole étudié ?*

### **Exercice 4 : Fenêtre en Réception**

On reprend le contexte de l'exercice précédent.

## Question 1

*Rappeler brièvement pour les protocoles de liaison le principe de la gestion des fenêtres en réception*

## Question 2

On suppose toujours que chaque émetteur peut utiliser au maximum  $\text{Maxseq}+1$  numéros de séquence différents numérotés de 0 à  $\text{Maxseq}$  (numérotation en modulo  $\text{Maxseq}+1$ ).

*Expliquer pourquoi la taille maximum de la fenêtre en réception doit rester inférieure à  $(\text{Maxseq}+1)/2$ .*

*Mettre en évidence un cas d'ambiguïté.*

*Indiquer pourquoi la taille de la fenêtre en réception ne peut être supérieure à la taille de la fenêtre en émission.*

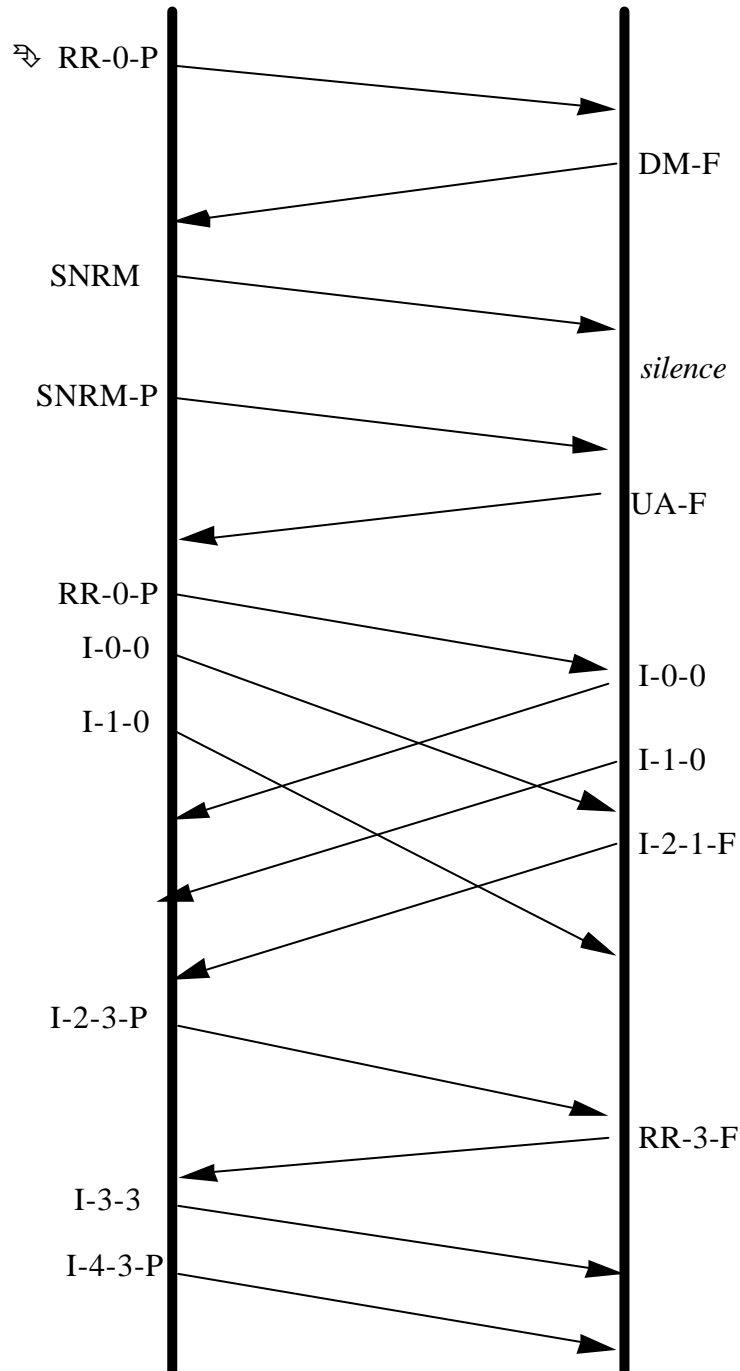
# 4• Niveau liaison (2)

## Protocoles de type HDLC

### Exercice 1 : Protocole à trames HDLC (cas disymétrique)

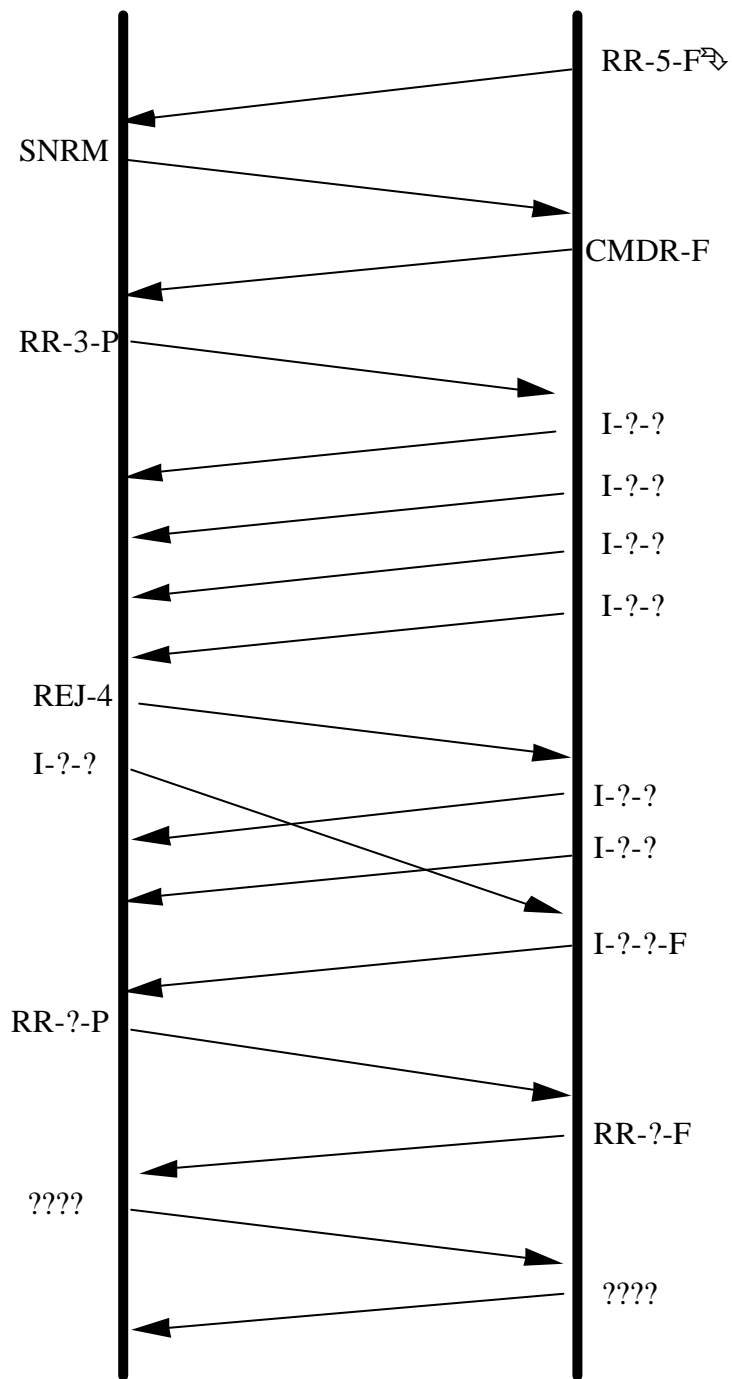
Commenter l'échange ci-dessous.

Chaque trame est spécifiée par TYPE - N(s) - N(r) - P/F.





Suite de l'échange :

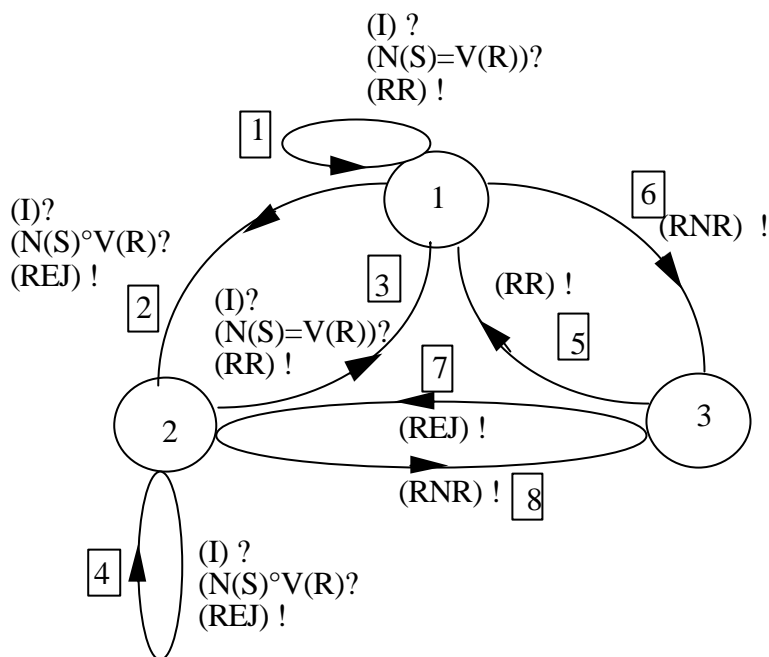


*Commenter les échanges*

*Compléter les champs des différentes trames*

## Exercice 2 : Automate d'états pour un protocole de type HDLC

Sur le diagramme d'automate suivant on note  $N(S)$  le numéro de séquence d'une trame d'information et  $V(R)$  le numéro de la trame attendue en réception. Sur chaque transition sont portées une trame reçue conditionnant le franchissement (suivi de ?), une trame émise (suivi de !) et une condition booléenne (suivi de ?).



### Question 1

*Que signifient les états 1, 2, 3 (symbolisés par des cercles) ?*

### Question 2

*Que signifient les transitions 1, 2, ... 8 (symbolisées par des rectangles) ?*

### Question 3

*Le protocole ne se comporte-t-il pas d'une façon surprenante du point de vue de l'état 3 ?*

*Proposer une modification de l'automate qui le rende plus cohérent.*

### Question 4

*Est-ce que le protocole utilise toutes les possibilités d'HDLC pour le contrôle de flux ?*

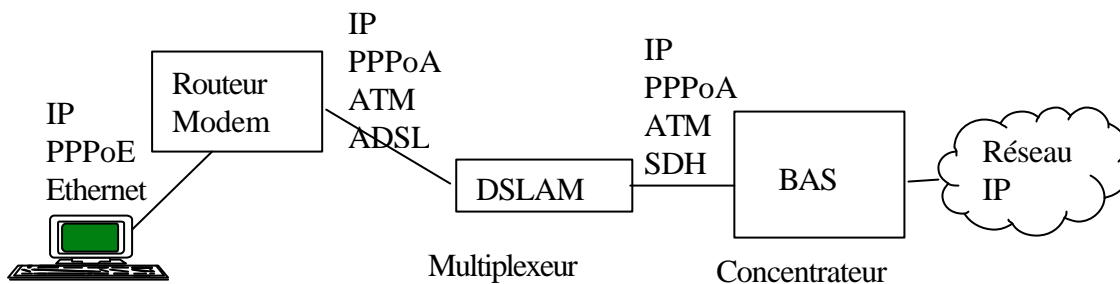
## Exercice 3 : Encapsulation PPP sur Ethernet pour ADSL

Dans ce problème on s'intéresse aux protocoles utilisés lors d'un accès à l'Internet par ADSL ('Asymmetric Digital Subscriber Line') et en particulier au protocole PPPoE (PPP on Ethernet).

### Question 1

Rappelez les principes généraux de la technologie ADSL au niveau physique ?

Le schéma suivant donne l'aperçu d'une architecture possible d'accès Internet avec ADSL en montrant les piles de protocoles utilisées.



- Le poste de travail d'un abonné ADSL fonctionne avec une pile de protocoles Internet. Nous supposons que le poste de travail est relié en Ethernet à un dispositif de raccordement ADSL (routeur/modem). Au niveau liaison, au dessus du protocole Ethernet, on utilise une version modifiée du protocole PPP, qui s'appelle pour Ethernet PPPoE (PPP over Ethernet).
- Le routeur/modem dans sa partie modem ADSL est connecté au réseau téléphonique. Au dessus du niveau physique ADSL, les données sont envoyées selon le protocole du réseau ATM. ATM 'Asynchronous Transfer Mode' est une architecture de réseau considérée comme de niveau 2. ATM implante toutes les fonctions de commutation d'un réseau en mode circuit virtuel pour des trames de petite taille (53 octets) qui sont baptisées cellules. De même au niveau liaison on utilise une version modifiée de PPP, qui s'appelle pour ATM PPPoA (PPP over ATM).
- Le routeur/modem dans sa partie routeur IP peut gérer plusieurs interfaces Ethernet ou des interfaces selon d'autres standards (USB ou Wifi). Dans notre exemple, le routeur recopie simplement les datagrammes IP circulant sur le réseau Ethernet, vers le multiplexeur de voies ADSL (le DSLAM) et réciproquement du DSLAM vers le réseau Ethernet.
- L'équipement DSLAM (en anglais 'Digital Subscriber Line Access Multiplexer') comporte pour chaque abonné un modem ADSL qui décode les informations au niveau physique ADSL. Le DSLAM est un équipement multiplexeur pour rattacher un ensemble d'abonnés. Il multiplexe les circuits virtuels ATM de chaque abonné sur une voie rapide jusqu'à un concentrateur d'accès au réseau Internet. Sur le schéma il est

mentionné que la voie rapide est gérée au niveau physique en SDH ('Synchronous Digital Hierarchy').

- Dans notre architecture, le concentrateur d'accès au réseau Internet (en anglais 'BAS Broadband Access Server') achemine les données vers le prestataire d'accès Internet de l'abonné. L'architecture du réseau Internet prestataire peut utiliser des voies de toute nature selon les choix prestataire et n'est pas décrite ici.

Pour le rattachement du poste de travail, qui se fait au niveau de l'utilisateur par une liaison Ethernet, une variante de PPP est utilisée. Au lieu de transmettre des trames PPP sur une liaison point-à-point, les trames PPP sont envoyées en réseau local dans une trame Ethernet. Cette encapsulation de PPP sur Ethernet, baptisée PPPoE pour PPP over Ethernet, est définie par la RFC 2516.

### **Question 2**

*Rappelez les fonctions du protocole PPP ?*

### **Question 3**

*Dans le fonctionnement habituel des réseaux Ethernet, il n'est pas prévu d'utiliser le protocole PPP au dessus du réseau Ethernet. Identifiez les fonctions du protocole PPP qui sont réalisées par le protocole Ethernet ?*

### **Question 4**

*Quand on examine en détail le protocole PPPoE on voit que les fanions de PPP sont supprimés. Pourquoi (comment les fanions sont-ils remplacés en Ethernet) ?*

### **Question 5**

*La trame PPP encapsulée en PPPoE ne comporte plus de zones adresse ni de zone contrôle. Finalement la trame PPPoE commence directement par la zone type de protocole utilisateur de PPP (par exemple PPPoE encapsulant de l'IP, ce qui est presque toujours le cas, cette valeur protocole vaut 21 en hexadécimal). Pourquoi les zones adresses et contrôle sont elles considérées comme inutiles en PPPoE?*

### **Question 6**

*Finalement, pourquoi les concepteurs de l'architecture d'accès Internet par ADSL ont jugé nécessaire de placer dans la pile des protocoles Internet le protocole PPPoE ?*

# 5• Ethernet

## Exercice 1 : Ingénierie des réseaux Ethernet

### Question 1 : réseau Ethernet 10 base T

*Comment fonctionne un répéteur Ethernet 10 base T (un « hub ») ?*

*Comment fonctionne un commutateur Ethernet 10 base T (un «lan switch») ?*

*Quelle est la différence de fonctionnement d'une carte ethernet en mode «Ethernet half duplex» et en mode «Ethernet full duplex» ?*

On rappelle que la trame Ethernet est précédée de 8 octets de synchronisation («préambule»), que la trame comporte au moins 64 octets d'informations significatives et que l'intervalle de temps qui sépare deux trames successives est d'au moins 9.6µs. Un commutateur Ethernet annonce dans sa publicité une performance par porte à 10 Mbit/s de 14 880 pps (paquet par seconde).

*Comment un acheteur peut-il interpréter cette annonce de performances ?*

### Question 2 : réseau "fast ethernet" (Ethernet 100 base T )

*Quelles sont les principales similitudes entre le réseau Ethernet 10 base T et le réseau Ethernet 100 base TX ?*

*Et les principales différences ?*

On rappelle que la taille minimum d'une trame Ethernet est de 64 octets. On suppose pour fixer les idées que la vitesse de propagation du signal dans le médium de communication ethernet est de 200000 km/s.

*Quelle est la distance maximum théorique qui peut séparer deux stations dans un réseau Ethernet 100 base T partagé (à base de répéteurs) ?*

Les distances effectivement recommandées sont de 90 mètres d'une station à un répéteur sur paires UTP5 avec possibilité de monter en cascade deux répéteurs séparés par 5 mètres de câble.

*Qu'est ce qui explique la différence entre la réponse à la question précédente et les valeurs effectives ?*

Certains standards spécifient des distances possibles d'utilisation de 2 kilomètres avec des fibres optiques.

*A quel type d'Ethernet correspondent de tels standards ?*

### Question 3 : Ethernet gigabit

Supposons qu'une taille minimum de 64 octets soit retenue pour un réseau Ethernet gigabit partagé et que la vitesse de propagation du signal soit de 200000km/s.

*Quelle est la distance maximum possible entre deux stations d'un réseau Ethernet gigabit ?*

La norme a prévu de rallonger la taille minimum de trame en la multipliant par 8 soit 512 octets (4096

bits) au lieu de 46 octets.

*Quelle est la distance possible entre deux stations du réseau ?*

## Exercice 2 : Etude d'un scénario de communication Ethernet

On considère un réseau local dont le partage de la voie est géré selon un algorithme CSMA/CD 1-persistant. La retransmission en cas de collision est effectuée selon l'algorithme du retard exponentiel binaire tronqué.

Ce réseau gère les transmissions entre 4 stations A, B, C et D.

Dans ce problème on utilise comme mesure de temps le "slot time". Les délais d'espacement intertrames ainsi que les durées de détection de voie libre sont négligés. Le temps de détection de collision est égal à 1 slot.

A l'instant  $t = 0$  la station A acquiert la voie et commence à transmettre un message.

A l'instant  $t = 5$  les stations B, C, et D reçoivent une demande de transmission de message.

Puis, pendant toute la durée considérée dans l'exercice aucune autre demande de transmission n'est soumise aux stations.

Tous ces messages sont de taille fixe et la durée de leur transmission est égale à 6 slots.

L'algorithme du retard binaire est implanté de la façon suivante :

```
Binary_backoff(attempts)
begin
  if attempts = 1 then
    maxbackoff := 2
  else
    if attempts = 10 then
      maxbackoff := backofflimit
    else
      maxbackoff := maxbackoff * 2
    endif
  endif
  delay := int (random * maxbackoff)
  Wait (delay * slot_time)
end
```

`attempts` est le nombre de tentatives pour accéder à la voie y compris celle en cours.

`backoff_limit` vaut  $2^{10}$

`int` est une fonction qui rend la valeur entière par défaut

`random` est un générateur de nombres aléatoires compris entre 0 et 1.

Dans l'exemple on considèrera que la fonction `random` rend successivement pour chaque station les valeurs données par le tableau suivant :

Station	B	C	D
1er tirage	1 / 2	1 / 4	3 / 4
2e tirage	3 / 4	1 / 6	5 / 8
3e tirage	1 / 3	2 / 3	1 / 2

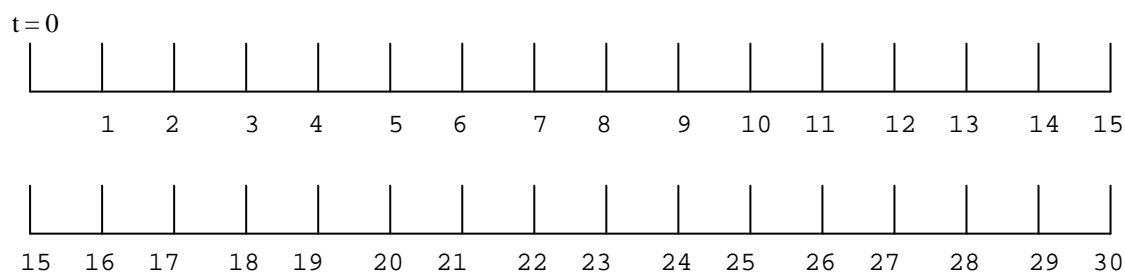
### Question 1

Compléter le diagramme suivant en indiquant pour chaque slot l'état de la voie.

Un slot occupé par la transmission d'un message correctement émis par la station A est représenté par "A"

Un slot occupé par une collision est représenté par "X"

Un slot correspondant à une absence de transmission est représenté par "—"



### Question 2

Calculer le taux d'utilisation de la voie sur la période allant de  $t = 0$  à la fin de la transmission du dernier message.

# 6• Installation de réseaux

## Ethernet partagés

Lors du déploiement d'un réseau Ethernet partagé on doit se préoccuper de la topologie du réseau afin de maintenir le diamètre de collision dans certaines limites.

### Question 1

*En Ethernet partagé qu'est ce qu'un domaine de collision? On caractérise le diamètre de collision par le temps d'aller-retour ('round trip delay'), pourquoi?*

### Question 2

Les informations que l'on utilise pour étudier une topologie Ethernet partagée incluent:

- le type des segments Ethernet utilisés (coaxial 10 Base 5, paire torsadée 10 Base T, fibre optique 10 Base FL, ...),
- la longueur des segments,
- la topologie d'ensemble des répéteurs et des segments.

Un réseau est correctement construit s'il respecte certaines règles concernant son domaine de collision. On peut utiliser la règle simple des 5 segments et 4 répéteurs au plus entre deux stations. A cette règle sont associées des précisions restrictives concernant les types et les tailles des segments mais les coefficients de sécurité appliqués sont importants. Dans certains cas cette règle s'avère insuffisante. Il est indispensable de faire un calcul précis, soit parce que le nombre de répéteurs et de segments est élevé (gros réseau), soit parce que la longueur des segments est importante (extension géographique grande).

La norme de base Ethernet IEEE 802.3 propose une méthode de calcul des délais de propagation très détaillée mais très complexe. Le groupe de travail sur les réseaux locaux IEEE 802.3 a proposé ensuite une méthode simplifiée mais néanmoins précise. Cette méthode, que nous allons étudier maintenant, est définie pour tous les réseaux Ethernet (10 Mb/s, 100 Mb/s, 1000 Mb/s).

On considère ici pour simplifier le cas des réseaux Ethernet à 10 Mb/s. Dans la méthode pour déterminer si un réseau est correctement construit, les calculs à réaliser expriment les délais en bits. En fait chaque bit transmis sur un réseau Ethernet étant associé à un certain délai de propagation au débit nominal considéré (ici 10 Mb/s), on considère qu'il y a équivalence entre mesurer un temps et mesurer un nombre de bits.

*Comment a été définie la tranche canal ('slot time') ? Quelle est sa durée ?*

*Si l'on se base sur la durée de la tranche canal, quel est le nombre de bits qui permet de mesurer le diamètre de collision ?*

### Question 3

En fait la trame Ethernet 10 Mb/s comporte un préambule utilisable également dans la détection des collisions puisqu'il rallonge la trame. Ce n'est plus vrai dans les normes 100 Mb/s ou 1000 Mb/s qui utilisent d'autres techniques de codage et de synchronisation.

*Dans le cas du réseau à 10 Mb/s si l'on réunit le préambule et la trame pour*

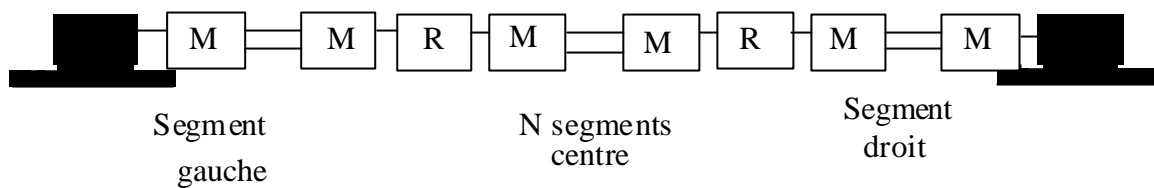


*définir la partie utilisable dans la détection des collisions, quel est le nombre de bits associé diamètre de collision ?*

La norme recommande d'introduire une sécurité supplémentaire de 5 temps bit pour ne pas trop s'approcher de la limite.

*Quel est le résultat final?*

Pour faire le calcul on doit tout d'abord déterminer le couple de stations connectées au réseau qui sont les plus éloignées (le pire des cas). On considère ensuite que ces stations sont interconnectées au moyen de répéteurs et de segments de trois types: un segment gauche, un ou plusieurs segments au centre et un segment droit. Pour chaque segment on fait apparaître sur le dessin qui suit, les câbles d'attachement (câbles 'drop') notés par un trait simple, les MAU (transmetteurs) représentés par une boîte avec la lettre M et le médium noté par un double trait. Les segments sont connectés par des répéteurs représentés par une boîte avec la lettre R.



**Figure 1. Modèle d'interconnexion entre deux stations**

#### **Question 4**

*Rappeler brièvement les définitions des différents organes présents dans la chaîne de la figure ci-dessus : interface AUI, câble d'attachement (câble 'drop'), transmetteur MAU, médium, répéteur ('hub')*

#### **Question 5**

Le tableau suivant représente pour les quatre types principaux de segments Ethernet (10 Base 5, 10 Base 2, 10 Base T, 10 Base FL) et pour le câble d'attachement les délais de propagation. En fait on y trouve :

- la longueur maximum en mètres,
- pour les trois positions possibles de segments (gauche, centre, droit), le nombre de bits pour un segment de base (segment de longueur minimum que l'on considère nulle),
- le nombre de bits pour un segment de longueur maximum

Pour des longueurs intermédiaires entre valeur de base et valeur maximum, le nombre de bits est linéaire en fonction de la longueur.

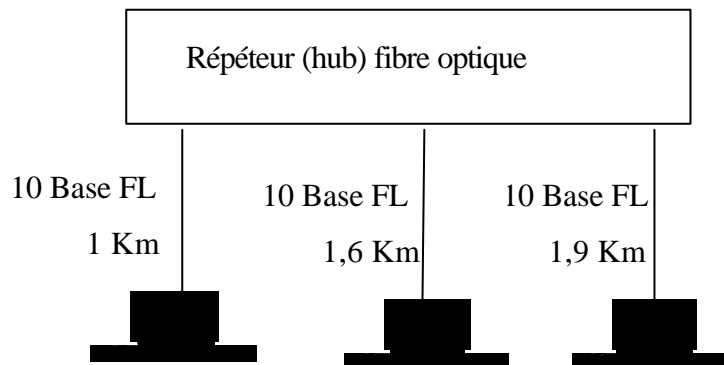
		Segment gauche		Segment centre		Segment droit	
Type	Lg Max	Base	Max	Base	Max	Base	Max
10 Base 5	500	11,75	55,05	46,5	89,8	169,5	212,8
10 Base 2	185	11,75	30,731	46,5	65,48	169,5	188,48
10 Base T	100	15,25	26,55	42	53,3	165	176,3
10Base FL	2000	12,25	212,25	33,5	233,5	156,5	356,5
Attachement AUI	48	0	4,88	0	4,88	0	4,88

**Figure 2. Tableau des valeurs en nombre de bits**

On remarque que les retards dus aux répéteurs n'apparaissent pas. Ils sont intégrés aux valeurs définies pour les segments (la valeur associée à un segment intègre dans le calcul réalisé par les IEEE tout ce qui concerne ce segment et ses répéteurs d'extrémité). Le cas des câbles d'attachement fait l'objet d'un traitement particulier. S'ils sont d'une longueur de base les retards pour ces câbles sont intégrés aux segments. S'il sont d'une longueur quelconque il faut rajouter une valeur comprise entre 0 (câble de base) et 4,88 bits (longueur de 48 mètres).

On remarque aussi sur le tableau que les valeurs ne sont pas les mêmes selon que le segment est à droite, au centre ou à gauche. Ceci est en relation avec la méthode employée pour intégrer les différents délais. Ces différences n'ont pas d'importance pour les segments centre et aussi pour le cas où les segments extrémités sont les mêmes. Si les segments extrémités ne sont pas identiques, comme l'analyse du diamètre de collision doit concerner le cas le plus défavorable, il faut faire deux calculs en échangeant les segments extrémités.

Sur la figure ci-dessous on a représenté un réseau Ethernet assez simple mais assez étendu géographiquement.



**Figure 3. Exemple de topologie Ethernet partagée**

*Est ce que le réseau Ethernet de la figure précédente est correctement construit ?*

*Dessiner le modèle de l'interconnexion entre stations pour ce réseau dans le cas le plus défavorable.*

*Calculer le diamètre de collision et conclure.*

On suppose que les transmetteurs optiques sont dans les stations et que les câbles d'attachement AUI sont de longueur de base.

### Question 6

On considère maintenant le réseau de la figure ci-dessous qui comporte cinq segments et quatre répéteurs Ethernet.

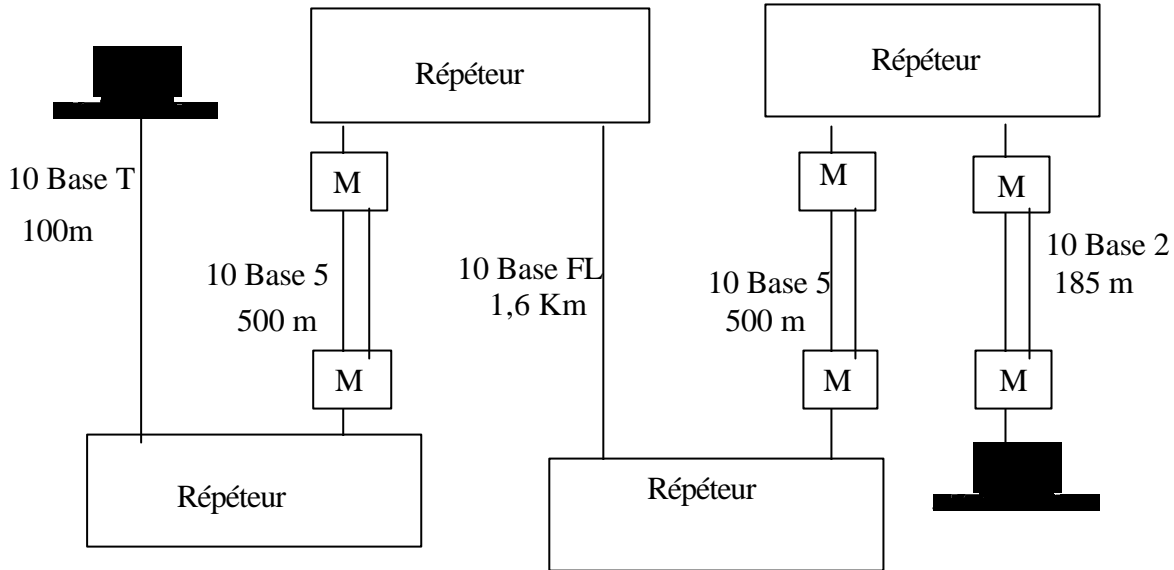


Figure 4. Exemple de topologie Ethernet partagée

Est ce que le réseau Ethernet de la figure 4 est correctement construit ?

On supposera que si des longueurs de câble ne sont pas précisées on prend le pire des cas.

### Question 7

Un autre problème se pose pour déployer correctement un réseau Ethernet, c'est de respecter le délai Inter trame de 9,6 microsecondes ('Interframe Spacing'). Ce délai est indispensable pour permettre aux appareils Ethernet de séparer correctement les trames. On offre ainsi un délai de relaxation qui permet aux équipements de terminer le traitement d'une trame avant de passer à la suivante. Or quand les trames traversent des équipements successifs qui ont des temps de réponse différents ou qui effectuent une reconstruction du signal (comme les répéteurs) il en résulte un raccourcissement apparent de l'intervalle inter trame (baptisé en anglais 'Interframe Gap Shrinkage'). Si ce rétrécissement est trop grave, les trames successives ne sont plus distinguées et on perd des trames car les contrôleurs considèrent que deux trames successives n'en font qu'une. La norme définit que le délai inter trame peut être raccourci jusqu'à 4,7 microsecondes sans risque. Au delà on estime que le réseau est mal construit.

Pour évaluer le raccourcissement on découpe le réseau selon les mêmes règles que précédemment et on évalue encore le raccourcissement en nombre de bits. On ne distingue plus que deux types de segments : segment de coaxial et autre segment. Par ailleurs on comptabilise seulement le segment gauche (celui sur lequel la trame est émise) et tous les segments milieu. Le segment droit ne participe pas au bilan global. Le tableau ci-dessous définit les valeurs de raccourcissement du délai inter trame en bits.

Type de segment	Segment gauche	Segment milieu
Coaxial	16	11
Autre	10,5	8

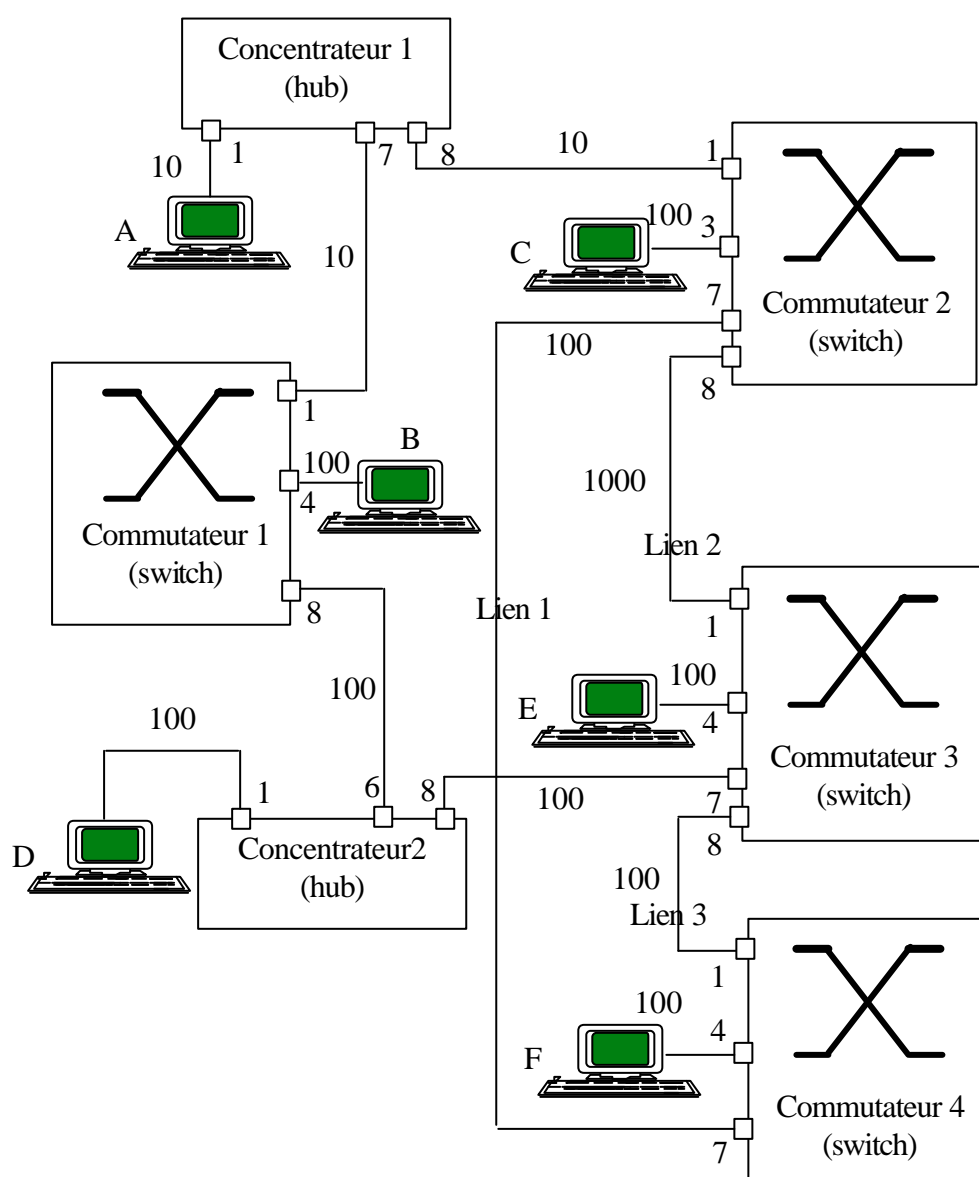
Figure 5. Raccourcissement du délai inter-trame

*Est ce que le réseau Ethernet de la figure 3 est correctement construit du point de vue du raccourcissement du délai inter trame ?*

*Même question avec le réseau de la figure 4*

# 7• Routage dans les commutateurs de réseaux locaux

Un ingénieur réseau reprend l'administration d'une architecture de réseau local ou tout fonctionne en Ethernet. L'architecture est constituée de quatre commutateurs ('lan switches') numérotés 1, 2, 3, 4 et de deux concentrateurs ('hubs') selon la figure suivante. Les commutateurs sont configurés en fonctionnement transparent avec l'algorithme de l'arbre couvrant ('spanning tree'). Pour chaque appareil, ont été mentionnés les numéros des ports utilisés pour l'interconnexion. L'architecture mentionne aussi trois tronçons Ethernet servant de liaison entre commutateurs (lien 1, 2, 3) ainsi que quelques stations de travail. Pour chaque voie de communication Ethernet on a mentionné son débit soit 10Mb/s soit 100 Mb/s soit 1000 Mb/S.



Les ports des commutateurs qui sont utilisés, sont numérotés sur la figure. La consultation des tables de configuration dans les commutateurs donne les informations suivantes :

**Commutateur 1 (Adresse MAC 00:A0:D6:13:43:65 Priorité 8000)**

Numéro du port	Adresse MAC du port	Priorité du port
Port 1	00:A0:D6:13:43:65	8000
Port 4	00:A0:D6:13:43:69	8000
Port 8	00:A0:D6:13:43:73	8000

**Commutateur 2 (Adresse MAC 00:A0:D6:14:37:E1 Priorité 8000)**

Numéro du port	Adresse MAC du port	Priorité du port
Port 1	00:A0:D6:14:37:E1	8000
Port 3	00:A0:D6:14:37:E4	8000
Port 7	00:A0:D6:14:37:E7	8000
Port 8	00:A0:D6:14:37:E8	8000

**Commutateur 3 (Adresse MAC 00:A0:D6:13:31:F6 Priorité 8000)**

Numéro du port	Adresse MAC du port	Priorité du port
Port 1	00:A0:D6:13:31:F6	8000
Port 4	00:A0:D6:13:31:F9	8000
Port 7	00:A0:D6:13:31:FC	8000
Port 8	00:A0:D6:13:31:FD	8000

**Commutateur 4 (Adresse MAC 00:A0:D6:09:18:12 Priorité 8000)**

Numéro du port	Adresse MAC du port	Priorité du port
Port 1	00:A0:D6:09:18:12	8000
Port 4	00:A0:D6:09:18:15	8000
Port 7	00:A0:D6:09:18:18	8000

### Question 1

Pour cette architecture, lorsque l'on fait fonctionner l'algorithme de l'arbre couvrant on élit un commutateur racine ('root switch').

*1.1) Qu'est ce qu'un commutateur racine ?*

1.2) *Comment est-il choisi ?*

1.3) *Quel est le commutateur qui est élu racine de l'arbre couvrant pour l'architecture donnée en exemple ?*

## **Question 2**

Pour chaque commutateur on élit un port racine ('root port').

2.1) *Qu'est ce qu'un port racine ?*

2.2) *Comment est-il choisi ?*

2.3) *Quels sont pour les quatre commutateurs les ports racine ?*

## **Question 3**

Pour chaque tronçon de réseau local ou voie de communication on élit un port désigné.

3.1) *Qu'est ce qu'un port désigné ('designated port') ?*

3.2) *Comment choisit-on un port désigné ?*

3.3) *Quels sont pour les différents tronçons les ports désignés ?*

## **Question 4**

*Après cette étude dessinez l'arbre couvrant construit automatiquement par l'algorithme de routage. Placez les commutateurs par niveaux en commençant par le commutateur racine, indiquez les ports racines par des cercles gris et les ports désignés par des carrés noirs, placez les stations ?*

## **Question 5**

*Comment fonctionne la construction des tables de routage. La table de routage peut-elle être indépendante de l'arbre couvrant construit ? Pourquoi ?*

## **Question 6**

*Quelle est la table de routage du commutateur 3 après une durée de fonctionnement suffisamment longue qui permet une connaissance complète du réseau et de son arbre couvrant ?*

## **Question 7**

*Finalement ce réseau vous paraît-il bien construit. Si non que proposez vous pour en améliorer le fonctionnement ?*

# 8• Gestion des adresses en IP

## Exercice 1 : Adressage IPV4 de base (hiérarchisé à deux niveaux).

L'adressage IPV4 a été créé dans sa version de base en distinguant trois classes d'adresses associées à trois classes de réseaux notés A, B et C.

- 1) *Comment est notée l'adresse d'un hôte et l'adresse d'un réseau ?*
- 2) *Comment un ordinateur hôte ou un routeur reconnaissent-ils qu'une adresse de destination appartient à l'une des classes ?*
- 3) *Quelle est la proportion relative du nombre d'adresses IPV4 affectées aux différentes classes A, B, C ? En déduire une conséquence si l'utilisation des adresses de classe A (ou B) est inefficace.*
- 4) *Quelle est l'opération effectuée sur une adresse de station pour déterminer son adresse de réseau ?*
- 5) *Comment l'adresse d'un hôte destinataire est-elle utilisée pour le routage ?*

On vient de voir que les conventions d'adressage de base IPV4 permettent implicitement la détermination de l'appartenance d'une adresse à l'une des classes A, B, C ainsi que celle de l'adresse du réseau auquel il appartient. Bien que cela ne soit pas nécessaire on souhaite maintenant pour toute adresse IP rendre explicite l'adresse de son réseau d'appartenance en utilisant systématiquement la notation 'adresse/n'. On rappelle que dans cette notation n est la longueur du préfixe définissant le réseau d'appartenance ou le nombre de bits en fort poids du masque.

- 6) *Quelle sont les valeurs de  $n_1$  et  $n_2$  pour les adresses suivantes : 17.234.16.45/ $n_1$ , 207.12.231.23/ $n_2$ .*
- 7) *Pourquoi a-t-on procédé à un tel découpage et quels en sont les difficultés actuelles ?*

## Exercice 2 : Adressage IPV4 de base avec la notion de sous réseau (hiérarchisé à trois niveaux).

L'adressage IPV4 a assez rapidement introduit la possibilité de structurer les adresses d'un réseau IP en sous réseaux. Une entreprise dont l'informatique était basée sur de petites architectures réseaux hétérogènes (Novell, ...) décide de passer à Internet. Après en avoir fait la demande l'entreprise a obtenu l'adresse 193.1.1.0. Compte tenu de l'organisation actuelle de l'entreprise l'ingénieur système doit définir au moins 6 sous-réseaux. Compte tenu de l'évolution prévisible de l'entreprise, l'ingénieur système pense que le sous-réseau le plus important peut comporter à moyen terme 25 hôtes.

### Question 1

*Quel est le découpage que doit effectuer l'ingénieur système ? En déduire la valeur du masque de sous réseau. On donnera le résultat dans la notation*



décimale pointée et dans la notation /n.

## Question 2

On considère le 2<sup>ème</sup> sous réseau dont l'adresse.

*Quelle est son adresse complète de sous réseau ?*

*Quelle est l'adresse de diffusion à tous les hôtes de ce sous réseau ?*

## Exercice 3 : Adressage en IPV4 avec CIDR

Comme son nom l'indique CIDR ('Classless Inter Domain Routing') est une approche sans classe. On ne considère plus une adresse comme appartenant implicitement à l'une des trois classes A, B ou C. En CIDR on associe explicitement à toute adresse de réseau IP un masque qui définit le préfixe qui caractérise le réseau auquel correspond cette adresse. Les adresses de réseaux sont donc maintenant toujours utilisées avec leur préfixe qui peut être de taille arbitraire (par exemple /8, /17, /21).

Supposons qu'on attribue à une entreprise l'adresse 194.16.0.0 avec le préfixe /21 soit en binaire un masque 11111111 11111111 11111000 0000000000 ou en notation décimale pointée une valeur de masque 255.255.248.0). Cette attribution veut dire que cette entreprise dispose pour son réseau du bloc d'adresse qui s'étend de 194.16.0.0 à 194.16.7.255. Soit l'adresse 194.16.6.23 d'un hôte dans ce réseau à atteindre. En utilisant le masque (défini ici par /21) qui doit toujours être associé à l'adresse on voit que cet hôte doit être atteint au moyen de l'adresse réseau 194.16.0.0. Il faut donc rechercher dans les tables de routage une entrée correspondant à cette adresse de réseau.

## Question 1

Considérons l'adresse CIDR d'un réseau qui serait 193.53.32.0/20.

*Quelle serait le nombre d'hôtes que comporterait ce réseau ?*

## Question 2

*Dans le réseau précédent 193.53.32.0/20 quelle est l'adresse la plus petite utilisable pour un hôte et quelle est la plus grande ?*

## Question 3

Supposons qu'un utilisateur restitue une ancienne adresse de classe A, B ou C comme 17.0.0.0 ou 134.15.0.0 ou 194.65.32.0 anciennement attribuées.

*Ces adresses n'étant plus jamais utilisées par leurs anciens propriétaires, pourrait-on les attribuer à nouveau selon l'approche CIDR (attribuer par exemple 17.46.64.0/19, 134.15.0.0/20 et 194.65.32.0/21) ?*

## Question 4

Une entreprise s'adresse à un Prestataire de Service Internet PSI (ISP 'Internet Service Provider') pour obtenir 800 adresses.

*Que devait faire le prestataire dans l'adressage par classes A, B, C pour satisfaire son client et avec quels inconvénients ?*

### Question 5

Nous supposons que le prestataire d'accès Internet a reçu pour exercer son activité le bloc d'adresses CIDR 202.0.64.0/18 avec lequel il a constitué son réseau. Chaque prestataire est libre de découper son espace d'adresse comme il l'entend pour fournir des adresses à ses clients. Les clients peuvent également à leur tour découper l'espace reçu pour le distribuer en interne selon les principes CIDR. Ils pourraient même devenir prestataires d'accès Internet.

*Pour un client demandant 800 adresses que va faire le prestataire si au moment de la demande la première adresse réseau qui est libre est 202.0.70.0 ?*

### Question 6

*Comment se passe avec CIDR le routage dans le réseau Internet pour atteindre l'un des hôtes appartenant au réseau du client ayant obtenu les 800 adresses ?*

*Vous prendrez si nécessaire une adresse à titre d'exemple dans cet ensemble.*

### Question 7

*En résumé montrez en quoi CIDR constitue une amélioration majeure de l'adressage IPV4.*

## Exercice 4 : Allocation d'adresses IP4 pour les réseaux privés

Dans le cadre du protocole IPV4 on a défini deux types d'adresses IP : les adresses IP publiques (également appelées globales) et les adresses IP privées (également appelées locales). Cette définition apparaît dans la norme RFC 1597 (mars 1994) dont le titre est 'Address allocation for private Internets' (version définitive RFC 1918 février 1996).

### Question 1

*Quelles sont les adresses IPV4 qui sont définies comme adresses privées (ou locales) et quelles sont les adresses qui sont définies comme publiques ou globales ?*

### Question 2

*Comment sont attribués ces deux types d'adresses ?*

### Question 3

*Comment sont utilisés ces deux types d'adresses (quelles sont les règles mises en oeuvre pour ces adresses dans un routeur d'un réseau IPV4 privé c'est à dire un réseau d'entreprise ou un réseau personnel et dans un routeur du réseau IPV4 global) ?*

### Question 4

*Dans quels buts a-t-on défini ces deux types d'adresses (avec quels avantages et quels inconvénients) ?*

## Exercice 5 : Traduction d'adresses IPV4 (NAT)

La norme RFC 1631 (mai 1994) ('The IP Network Address Translator'), définit un principe général de traduction d'adresses IP. La dernière version, la plus récente de cette approche RFC 3002 (janvier 2001) améliore différents points.

La traduction d'adresses peut être appliquée par différents types d'appareils dont la caractéristique principale est d'être situés entre un réseau IPV4 privé et le réseau IPV4 global. Typiquement la traduction est effectuée par un routeur, mais on peut aussi appliquer la traduction dans un hôte quelconque ou dans un filtre (pare-feu ou 'firewall').

La traduction au niveau des adresses IP s'applique à l'adresse source d'un datagramme IP en provenance du réseau privé (baptisé encore en NAT réseau interne) et à destination du réseau public (baptisé encore en NAT réseau externe). De manière symétrique, la traduction est effectuée sur les datagrammes en provenance du réseau public (ou externe) vers le réseau privé (ou interne).

La traduction d'adresse peut être réalisée de différentes façons qui sont examinées dans les questions suivantes.

### Question 1

Dans le mode NAT statique l'adresse IPV4 source privée est traduite en une adresse IPV4 source publique qui est toujours la même. La correspondance dans ce cas est bijective (biunivoque) c'est-à-dire qu'à une adresse privée est associée de manière statique une adresse publique (selon une table de correspondance statiquement définie par un administrateur réseau).

*Quelle utilisation peut-on faire d'un tel mode de traduction d'adresses IP ?  
Quels sont les inconvénients ?*

### Question 2

Dans le mode NAT dynamique, la traduction d'une adresse source IPV4 privée est effectuée vers une adresse source IPV4 publique qui est prise dans un bloc d'adresses publiques disponibles. L'adresse publique utilisée n'est donc pas toujours la même. Par exemple si l'on suppose que l'hôte d'adresse 172.20.40.17 émet un datagramme à un instant donné vers l'Internet global, son adresse est traduite dans la première adresse disponible d'un bloc. Par exemple, si l'adresse 212.19.50.63 du bloc disponible 212.19.50.0 à 212.19.50.255 est non utilisée au moment de l'émission du datagramme, on l'utilisera et on traduira 172.20.40.17 en 212.19.50.63. Cette correspondance est enregistrée dans une table. De manière à éviter de bloquer indéfiniment une adresse attribuée dynamiquement, un temporisateur est utilisé pour révoquer l'attribution d'une adresse publique. A l'échéance, on récupère une adresse attribuée et l'on procède à une nouvelle attribution d'adresse si un nouvel échange à lieu (éventuellement on peut reprendre la même adresse pour un autre quantum).

*Quel avantage nouveau obtient-on d'un tel mode de traduction d'adresses IP ?*

### Question 3

Le troisième mode est connu sous différents noms (mode NAT avec surcharge NAT 'overloading' encore appelé NAT with PAT 'Port Address Translation'). Dans ce cas la traduction

d'une adresse source IPV4 privée vers une adresse source IPV4 publique est complétée par la traduction du numéro de port. Le plus souvent, dans ce cas on suppose l'utilisation d'une seule adresse publique (par exemple une adresse publique comme 212.19.50.63 disponible). Si l'on suppose que l'hôte d'adresse 172.20.40.17 émet un datagramme selon le protocole TCP avec le numéro de port source 5032, alors son adresse IP est traduite en l'adresse IP publique (212.19.50.63) et le numéro de port source TCP est également traduit vers un numéro de port non utilisé (par exemple 4097 si ce port n'est pas déjà attribué à une autre communication). Comme dans le cas du NAT dynamique, les attributions sont associées à un temporisateur avec récupération à échéance. Ce mode de fonctionnement est le plus utilisé.

*Quels en sont les avantages et les inconvénients ?*

## Exercice 6 : NAT et voix sur IP

L'approche NAT ('Network Address Translation') présente dans le cadre du protocole IPV4 de nombreux avantages. NAT pose aussi différents problèmes avec certaines applications Internet en particulier des applications d'actualité comme les communications de voix sur IP (VoIP 'Voice over IP').

En communication de voix sur IP on cherche à réaliser des communications vocales en utilisant le réseau Internet. L'analogie du numéro de téléphone est une adresse IPV4 d'interface d'accès à un appareil (un poste de travail qui possède un micro et un écouteur ou un téléphone IP). Cependant il n'a pas été retenu d'utiliser directement des adresses IP pour désigner un correspondant comme on le fait des numéros de téléphone. On rappelle que l'attribution d'adresse IP peut être statique ou dynamique.

### Question 1

*On s'intéresse au cas d'une attribution statique des adresses IP. Un émetteur peut-il utiliser l'adresse IP directement pour appeler un correspondant comme on le fait avec un numéro de téléphone (justifiez votre réponse)?*

### Question 2

*On se place maintenant dans le cas d'une attribution dynamique (DHCP). Quel(s) problème(s) se posent en utilisation d'adresses IP dynamiques pour appeler un correspondant ?*

### Question 3

*Dans le cas où l'on se trouve dans un réseau privé avec un routeur NAT, peut-on directement utiliser les adresses IP pour appeler un correspondant comme on le fait avec un numéro de téléphone ?*

Dans les protocoles de voix sur IP on utilise une gestion d'annuaires. Les annuaires sont placés dans l'Internet public et accessibles en ligne en mode client-serveur. C'est le cas en SIP ('Session Initiation Protocol' un protocole de signalisation sur réseau IP) ou en SKYPE (système de téléphonie 'gratuite' utilisant la voix sur IP). Rappelez le rôle d'un serveur d'annuaire (quelles sont les trois opérations principales réalisées par un serveur d'annuaire ?).

### Question 4

*Dans le cas de la voix sur IP à quoi correspondent les noms logiques et les adresses physiques et à quel moment sont réalisées les opérations d'annuaire?*

### Question 5

Dans certains protocoles d'application de l'Internet, certains messages protocolaires contiennent l'adresse IP V4 source de l'émetteur dans l'entête du datagramme IP mais aussi dans la partie donnée du message (dans la charge utile). Par exemple, en voix sur IP, dans quel cas peut-on trouver une adresse IP dans un message?

*Quel problème pose l'utilisation de NAT pour de tels protocoles ?*

### **Question 6**

Différentes solutions ont été proposées pour résoudre le problème précédent (adresses IP dans une charge utile). Une solution consiste à faire en sorte que les applications qui font de la voix sur IP reçoivent des adresses IP fixes publiques ou des traductions en adresses IP fixes publiques.

*Discutez cette solution (évaluez les avantages et les inconvénients, la faisabilité de la solution) ?*

### **Question 7**

Une autre solution consiste à faire en sorte que les routeurs NAT connaissent la structure des messages des protocoles de voix sur IP comme SIP ou Skype.

*Précisez et discutez cette solution ?*

### **Question 8**

Une troisième solution consiste à utiliser un protocole client serveur baptisé STUN ('Simple Traversal of UDP Through NAT' RFC 3489 mars 2003). Ce protocole a été conçu pour répondre aux problèmes des adresses IP contenues dans la partie donnée des messages.

Un client STUN est un utilisateur de l'Internet qui souhaite connaître son adresse IP et son numéro de port. Un serveur STUN est situé dans l'Internet global (celui des adresses publiques). Il possède un port de numéro réservé (port 'bien connu'). Dans un message de requête un client STUN (typiquement un téléphone IP) émet une demande de son adresse IP et de son numéro de port vers un serveur STUN situé dans l'Internet global. Le serveur STUN analyse le datagramme reçu et répond en retournant au client l'adresse IP et le port public du client dans le message.

On se place dans le cas où les adresses sont traduites en sortie d'un domaine (traduction des adresses et port source sur les datagrammes en sortie et des adresses et ports destination sur les datagrammes en entrée). On fait l'hypothèse que le routeur NAT effectue toujours la même traduction pour tous les datagrammes ayant un couple adresse, numéro de port donné. Comment le serveur STUN peut-il connaître l'adresse IP et le numéro de port du demandeur dans l'Internet global?

*Expliquez comment le client utilise les informations reçues pour résoudre le problème des adresses IP contenues dans les messages ?*

### **Question 9**

De nombreux routeurs NAT effectuent une traduction d'adresse IP et de numéro de port source qui dépend de la destination. Tous les datagrammes ayant même source et même destination sont traduits de la même façon. Deux datagrammes ayant même source (adresse IP et numéro de port) et deux destinations différentes (adresse IP ou numéro de port) voient l'adresse IP et le numéro de port source traduits de deux façons différentes.

*Expliquez pourquoi dans ce cas, le protocole STUN ne marche plus.*

## Exercice 6 : Distribution d'adresses avec DHCP

DHCP ('Dynamic Host Configuration Protocol' RFC 2131 et 2132) est un protocole client serveur qui permet à un client hôte d'un réseau local (Ethernet ou Wifi) d'obtenir d'un serveur DHCP différents paramètres de configuration réseau. En utilisant DHCP on souhaite surtout fournir à un hôte une adresse IP mais aussi le masque du sous-réseau auquel appartient cet hôte, l'adresse IP du routeur par défaut ou encore l'adresse IP d'un serveur DNS. Pour attribuer des adresses IP, un serveur DHCP reçoit un ensemble d'adresses IP qu'il attribue ensuite sur demande à des clients pour une période de temps donnée. En DHCP on appelle bail le fait pour un hôte d'obtenir une adresse IP pour une période de temps définie par le serveur. Le protocole d'acquisition d'un bail comporte quatre messages principaux :

A - Le client DHCP émet en diffusion un premier message de demande de bail. Le type de ce message est baptisé DHCPDISCOVER.

B - S'il existe plusieurs serveurs DHCP atteints par la diffusion et si ces serveurs disposent d'une adresse IP libre, ces serveurs DHCP proposent au client cette adresse IP associée à une durée d'utilisation possible de l'adresse (une durée de bail). Ce message contient aussi l'adresse IP du serveur proposant l'offre. Le type de ce message de réponse est DHCPOFFER.

C - S'il a reçu plusieurs propositions, le client en choisit une et retourne une demande d'utilisation de cette adresse. Le type de ce troisième message est DHCPREQUEST. Ce message est également diffusé pour que les autres serveurs DHCP apprennent qu'ils n'ont pas été sélectionnés.

D - Le protocole se termine par la transmission d'un message DHCPACK par lequel le serveur DHCP sélectionné accuse réception de la demande et accorde l'adresse selon la durée de bail prévue. Les autres serveurs retirent définitivement leur offre.

A la moitié de la période d'utilisation d'une adresse (moitié du bail) le client demande le renouvellement de l'allocation de cette adresse par un message DHCPREQUEST. Le bail est généralement renouvelé par un DHCPACK. Si la demande n'aboutit pas (cas d'une réponse DHCPNACK ou perte de contact avec le serveur DHCP), le client tente de contacter les autres serveurs DHCP pour obtenir une autre adresse. En l'absence de réponse positive, le client utilise l'adresse dont il disposait jusqu'à la fin du bail et cesse de communiquer en IP.

Un analyseur de messages échangés sur un réseau local Ethernet/IP donne le résultat suivant. Il est constitué d'une suite de lignes correspondant à un message observé sur le réseau local. On trouve un numéro d'ordre du message observé, la date de l'observation en seconde, les adresses IP source et destination, le nom du protocole pour lequel le message a circulé et le type du message

No	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
2	0.001182	192.168.0.247	192.168.0.5	ICMP	Echo request
3	0.342454	192.168.0.247	192.168.0.5	DHCP	DHCP Offer
4	0.344405	0.0.0.0	255.255.255.255	DHCP	DHCP Request
5	0.348264	192.168.0.247	192.168.0.5	DHCP	DHCP ACK
6	0.353014	CIS_a8:52:24	Broadcast	ARP	Who has 192.168.0.5?
Tell	192.168.0.5				

### Question 1

*Pour le message numéro 1 de la trace expliquez la signification des adresses IP source et destination (pourquoi selon vous utilise t'on ces adresses dans cet échange) ?*

### **Question 2**

*La trace ne donne pas l'adresse MAC destination figurant dans le message numéro 1 (l'adresse MAC source correspond à l'adresse unique de l'émetteur). Même si elle ne figure pas dans le texte pouvez vous donner l'adresse destination ?*

### **Question 3**

*Pour le message numéro 3 de la trace expliquez la signification des adresses source et destination (à quoi correspondent ces adresses) ? Comment est il possible que ce message parvienne correctement à son destinataire ?*

### **Question 4**

*Pour le message numéro 4, expliquez la signification des adresses IP source et destination (pourquoi avoir choisi les adresses IP qui apparaissent dans le message 4)?*

### **Question 5**

*Dans cette trace, le message numéro 2 semble ne pas être relié à une attribution d'adresse DHCP. Cependant ce message a circulé aussi dans le cadre de l'attribution d'adresse. Pourquoi le message numéro 2 a-t-il circulé (quel est le but poursuivi dans la circulation de ce message) ?*

### **Question 6**

*Expliquez pourquoi le temps qui s'écoule entre les messages 2 et 3 est assez long ?*

### **Question 7**

*De la même façon, décrivez pourquoi le message 6 a circulé dans cette trace?*

Un administrateur réseau installe un serveur DHCP sur une machine UNIX. Dans son implantation il doit configurer le serveur par un ensemble de directives contenues dans un fichier baptisé dhcpd.conf. La liste des directives préparées pour une configuration est la suivante :

```
default-lease-time 600;

max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1,192.168.1.2;
option domain-name "mondomaine.org";

subnet 192.168.1.0 netmask 255.255.255.0
{
  range 192.168.1.10 192.168.1.100;
  range 192.168.1.150 192.168.1.200;
}
```



```
host ulysse
{
hardware ethernet 00:19:18:A6:47:36 ;
fixed-address 192.168.0.10;
}
```

### **Question 8**

*Les adresses IP attribuées par ce serveur DHCP correspondent à un choix particulier. A quelle catégorie appartiennent ces adresses ?*

### **Question 9**

*On constate dans le fichier de configuration dhcpd.conf deux types de directives d'allocation d'adresses IP. Dans le cas de la machine ulysse, celle-ci reçoit toujours la même adresse IP fixe (voir la ligne 'fixed-address 192.168.0.10'). Citez les avantages que vous voyez à l'utilisation de DHCP dans ce cas ?*

### **Question 10**

*Dans le cas du sous réseau 192.168.1.0 l'administrateur définit des plages d'adresses attribuables dynamiquement (dans les directives range comme range 192.168.1.10 192.168.1.100;). Pourquoi préciser de telles plages d'adresses et quels avantages en tire t'on ?*

## Exercice 7 : Utilitaire ping et adresses IPV6

L'utilitaire ping créé pour le protocole IPV4 a été adapté à IPV6. Il s'appelle alors ping6. Sur une machine, l'exécution de la commande ping6, donne une liste résultat de la forme suivante :

```
$ ping6 2001:660:3003:1D05::1:1

PING ping6 2001:660:3003:1D05::1:1: 56 data bytes

64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=0 time=43.1 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=1 time=40.0 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=2 time=44.2 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=3 time=43.7 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=4 time=38.9 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=5 time=41.2 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=6 time=39.1 ms
64 bytes from 2001:660:3003:1D05::1:1: icmp_seq=7 time=42.1 ms

- --- 2001:660:3003:1D05::1:1 ping statistics ---

 9 packets transmitted, 9 packets received, 0% packet loss

round-trip min/avg/max = 38.9/41.3/44.2 ms
```

### Question 1

*Comment fonctionne l'utilitaire ping. Que peut-on déduire du résultat de l'exécution de cette commande ?*

### Question 2

L'adresse IPV6 utilisée en paramètre de la commande ping6 est l'adresse 2001:660:3003:1D05::1:1 . Il s'agit d'une adresse notée sous une forme compacte (avec des raccourcis).

*Quelles sont les règles définies pour compacter une adresse IPV6. Comment se note l'adresse 2001:660:3003:1D05::1:1 sous une forme développée (notation complète d'une adresse IPV6) ?*

### Question 3

*A quelle catégorie (à quel plan d'adressage) appartient l'adresse 2001:660:3003:1D05::1:1 (selon son préfixe est-ce une adresse prestataire, agrégée ou géographique). Même question pour l'adresse: 5F0D:E900:80DF:E000:0001:0060:3E0B:3010 ?*

### Question 4

*Commentez la valeur des temps d'aller retour (round trip time) (que pouvez vous dire à la lecture de ces chiffres) ?*

## Exercice 8 : Mobilité avec IP en version 4

Les appareils portables (comme les ordinateurs portables, les téléphones IP, les organiseurs...) qui utilisent les protocoles de l'Internet, posent le problème du déplacement d'un hôte IPV4 à l'intérieur de l'Internet. L'objectif de la norme 'IP Mobility' (RFC 3344 dernière version en 2002) encore connue sous le sigle MIP4 (pour 'Mobile IP' en version 4) est de permettre à un hôte dans un réseau IP de changer de point de rattachement au réseau Internet en conservant toujours la même adresse IP.

L'adressage IPV4 fait que tout appareil doit posséder une adresse IP qui permet de le localiser dans un réseau auquel il est rattaché. IP mobile en V4 a donc comme objectif de permettre à un hôte de communiquer avec d'autres hôtes dans le réseau Internet même après un changement de point d'attachement sans avoir à reconfigurer manuellement cet hôte. La norme IP mobile suppose donc qu'un ordinateur mobile (un nœud mobile ou 'mobile node' en anglais) possède une adresse IP principale fixe qui appartient à son réseau d'origine (son réseau 'home network'). C'est avec cette adresse IP qu'il doit continuer de pouvoir être accessible en toutes circonstances qu'il soit connecté dans son réseau d'origine ou qu'il se soit déplacé dans un réseau étranger ('foreign network').

Pour les besoins de la mobilité, IP mobile en version 4 fait l'hypothèse qu'un hôte mobile doit être modifié pour supporter un ensemble de logiciels réseaux spécifiques lui permettant d'être mobile (en particulier la couche IP est modifiée). Nous allons voir que certains routeurs doivent également subir des modifications en vue de la mobilité. Par contre un hôte habituel de l'Internet qui communique avec un mobile (en anglais 'correspondent node') doit rester un hôte quelconque de l'Internet c'est-à-dire qu'il ne doit pas avoir à subir de modifications de ses logiciels réseaux Internet.

Pour assurer la mobilité en IP, une première solution consisterait à utiliser le routage IP. Il faudrait définir dans les tables de routage, des routes vers des hôtes (en anglais 'host specific route') de sorte qu'un hôte mobile dans le réseau Internet pourrait conserver toujours la même adresse IP tout en restant accessible n'importe où dans l'Internet grâce au routage IP.

### Question 1

*Etudiez la solution de mobilité en IP par l'utilisation de routes conduisant vers un hôte unique. Quelles seraient les conséquences d'une telle approche de la mobilité sur le fonctionnement de l'Internet?*

Indications : vous examinerez les avantages et les inconvénients de cette solution en considérant principalement les problèmes de performances des opérations à réaliser que sont la commutation d'un datagramme dans un routeur et la mise à jour des routes par les protocoles de routages dynamiques compte tenu de l'existence de routes vers les hôtes uniques.

### Question 2

*On se place maintenant dans l'hypothèse ou lorsqu'un mobile arrive dans un réseau étranger, il communique en IP en utilisant une adresse IP dans ce réseau. En IP mobile cette nouvelle adresse est baptisée 'care-of address'. Citez toutes les techniques que vous connaissez permettant à un hôte, d'obtenir dynamiquement une adresse IP dans un réseau ?*

Lorsqu'un mobile est arrivé dans un réseau étranger nous supposons qu'il dispose d'un moyen pour s'apercevoir qu'il a changé de réseau. Par exemple, en interrogeant un serveur sur la valeur du préfixe réseau courant il peut déterminer s'il a changé de réseau. Nous supposons que le mobile demande alors et obtient une adresse IP dans ce réseau par l'un des moyens listés à la question précédente.

### Question 3

*Quelles sont les possibilités de communications Internet qui sont offertes au mobile au moyen de cette nouvelle adresse (l'adresse dans le réseau étranger)?*

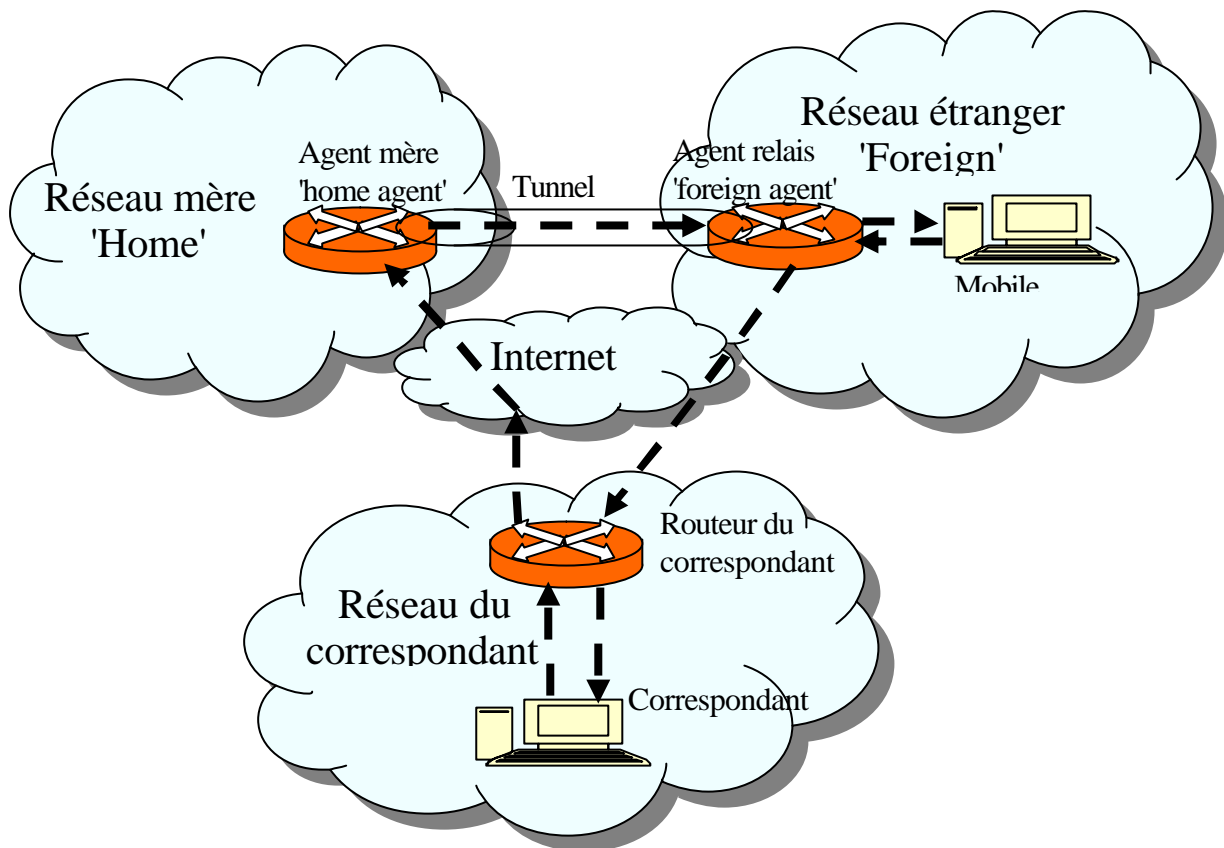
Indications : peut-il appeler un nouveau correspondant ? Peut-il continuer une communication qui était en cours avec un correspondant malgré le changement d'adresse (justifiez votre réponse en particulier si le transport utilisé est TCP) ? Peut-il être appelé par un nouveau correspondant ?

Pour permettre à un correspondant d'envoyer des datagrammes vers un mobile, IP mobile suppose l'existence de deux systèmes informatiques jouant des rôles particuliers. Le plus souvent il s'agit d'extensions logicielles en vue de la mobilité qui sont installées dans des routeurs.

L'agent mère (traduction la plus fréquemment constatée de 'home agent') est situé dans le réseau mère c'est-à-dire le réseau d'origine du mobile ('home network'). C'est très souvent le réseau de l'entreprise où travaille la personne qui utilise un mobile de façon professionnelle. Le rôle de l'agent mère ('home agent') est de remplacer un mobile dans son réseau d'origine lorsque celui-ci est absent. L'agent mère reçoit les datagrammes IP adressés au mobile sur son adresse IP principale et les réexpédie vers le mobile dans un autre réseau où celui-ci s'est déplacé.

L'agent relais ('foreign agent') est situé dans le réseau étranger visité par le nœud mobile (en anglais le 'foreign network'). Il doit enregistrer la présence du mobile et sa nouvelle adresse IP lorsqu'il vient d'arriver dans le réseau étranger. Mais son rôle est principalement de recevoir les datagrammes retransmis par l'agent mère et de les relayer pour les délivrer à destination du mobile. Il lui faut aussi signaler à l'agent mère son adresse d'agent relais pour que l'agent mère puisse lui réexpédier les datagrammes arrivés pour le mobile. Dans le sens inverse, le mobile répond aux datagrammes qui sont envoyés par un correspondant en s'adressant directement à ce correspondant.

En raison de l'existence de ces trois entités essentielles au fonctionnement du routage IP mobile (un correspondant avec son routeur de rattachement, un agent mère dans le réseau mère et un agent relais dans le réseau étranger) le routage d'un datagramme en IP mobile est baptisé routage triangulaire. La figure suivante traduit la circulation des datagrammes IP du correspondant vers le mobile et du mobile vers le correspondant. On peut voir une grande analogie entre ce fonctionnement pour les datagrammes et la réexpédition du courrier postal.



#### Question 4

*On rappelle qu'avec IP mobile, un mobile est toujours atteint au moyen de son adresse IP de rattachement dans son réseau mère (son réseau principal d'accueil 'home'). Comment l'agent mère peut-il faire pour remplacer un mobile IP quand celui-ci est absent de ce réseau d'origine ?*

Indications : Recherchez le protocole permettant à un hôte d'un réseau IP de se déclarer destinataire des messages à destination d'une certaine adresse IP.

L'agent mère ayant récupéré tous les datagrammes à destination du mobile, doit les retransmettre au mobile qui se trouve dans le réseau étranger par l'intermédiaire de l'agent relais. Mobile IP impose que la communication entre l'agent mère dans le réseau mère et l'agent relais dans le réseau étranger s'effectue en mode tunnel. Utiliser un tunnel signifie que le datagramme IP qui avait été transmis d'un correspondant vers le mobile est encapsulé dans un nouveau datagramme IP. On conserve donc toute l'entête d'origine et toute la charge utile du datagramme original en considérant le tout comme la charge utile d'un nouveau datagramme avec une nouvelle entête IP entre agent mère et agent relais. L'agent relais peut donc récupérer en sortie du tunnel, le datagramme transmis initialement par le correspondant et c'est ce datagramme qui est utilisé pour la délivrance au mobile dans le réseau étranger.

#### Question 5

*Pourquoi procède t'on ainsi ?*

# 9• Fonctionnement d'IP

## Exercice 1 : Fragmentation IP

### Question 1

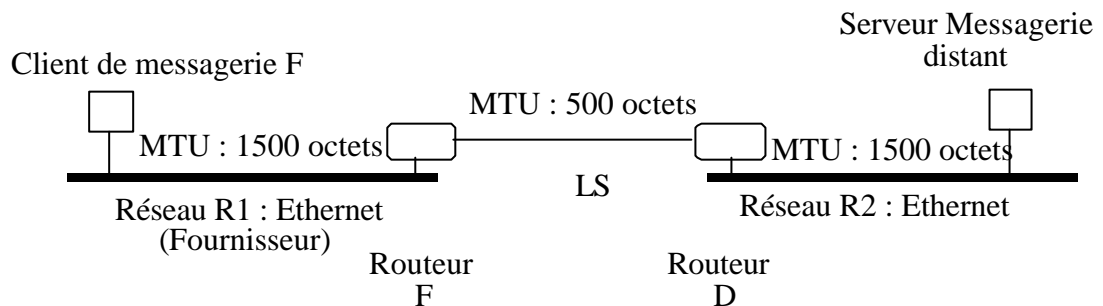
*Dans un réseau qu'est ce que la fragmentation?*

### Question 2

*Comment fonctionne la fragmentation en IP V4 (expliquez en les principes généraux) ?*

### Question 3

Un client de messagerie F transfère un message électronique de 4000 octets de données vers un serveur distant en utilisant trois voies de communication successives selon la figure ci-après. On considère que toutes les entêtes ajoutées par les différentes couches de protocoles traversées au dessus de la couche IP font partie des 4000 octets. Dans les datagrammes IP l'entête est une entête standard de 20 octets (il n'y a pas d'options rajoutées en extensions dans les entêtes IP).



*Expliquez dans les grandes lignes le fonctionnement de la fragmentation dans ce cas.*

*Combien de datagrammes sont échangés, où sont-ils créés?*

### Question 4

*Pour l'exemple précédent décrivez précisément les entêtes des datagrammes IP échangés. Vous ne décrirez que les champs associés à la fragmentation et la longueur du datagramme ?*

## Exercice 2 : Principe de base du routage dans le réseau Internet

Dans un routeur IP la table de routage comporte pour chaque entrée une route. On trouve dans l'exemple de la table suivante:

- un numéro d'entrée pour se repérer facilement,
- l'adresse de destination,
- le masque de réseau de l'adresse destination (en notation /n),
- l'adresse IP du prochain routeur ou du prochain hôte à visiter sur la route,
- le coût (la métrique).

D'autres informations sont prévues dans les tables de routage IP mais n'apparaissent pas dans l'exemple comme l'adresse du port à utiliser en sortie ou le type de la route pour définir si le datagramme IP doit atteindre une destination distante ou s'il est à délivrer à sa destination par le présent routeur.

N°	Destination	Masque	Routeur	Métrique
1	0.0.0.0	/0	10.1.3.65	1
2	10.1.0.0	/16	10.1.3.65	1
3	10.1.3.0	/26	10.1.3.1	0
4	10.1.3.64	/26	10.1.3.126	0
5	10.1.3.128	/26	10.1.3.190	0
6	10.1.3.192	/26	10.1.3.254	0
7	10.1.4.0	/26	10.1.3.4	11
8	10.1.4.64	/26	10.1.3.4	9
9	10.1.4.128	/26	10.1.3.4	10
10	10.1.16.64	/26	10.1.3.65	5
11	10.1.8.0	/24	10.1.3.65	6
12	10.1.8.0	/26	10.1.3.65	9
13	10.1.8.64	/26	10.1.3.65	17
14	10.1.8.64	/26	10.1.3.62	22
15	10.1.8.128	/26	10.1.3.65	25

### Question 1

*Rappeler le test à appliquer à chacune des entrées de la table pour déterminer parmi celles-ci quelles sont celles qui correspondent à des routes permettant d'atteindre une destination donnée. Application à la destination 10.1.8.66.*

*Quelles sont les routes qui passent positivement le test ?*

## Question 2

Lorsque l'on a opéré ce premier élagage on réalise un second élagage conduisant à choisir les routes qui sont associées aux masques les plus longs.

*Pourquoi les routeurs doivent-ils réaliser une recherche de "correspondance la plus longue" ('Longest Match based forwarding algorithm') ?*

*Donner le numéro des entrées qui passent ce second filtrage.*

## Question 3

Les routeurs peuvent ensuite arbitrer entre différentes routes selon un routage de la pomme de terre chaude. Dans le paquet IP il existe dans l'entête une zone dédiée à la qualité de service du paquet (TOS 'type of service'), qui contient deux informations. Rappelez la signification de ces deux informations de qualité de service.

*Que peut faire un routeur pour utiliser cette zone et filtrer entre les différentes routes encore jugées équivalentes?*

## Question 4

Un quatrième filtrage peut utiliser la métrique.

*Rappeler la signification de cette valeur.*

*Comment utiliser cette entrée dans la table de routage pour filtrer entre les différentes routes qui seraient encore jugées équivalentes ?*

## Question 5

Un cinquième filtrage peut mettre en avant des techniques propres à chaque fabricant de routeur.

*Quelle optimisation plus globale au réseau peut-on encore réaliser si l'on a encore plusieurs routes jugées équivalentes ?*

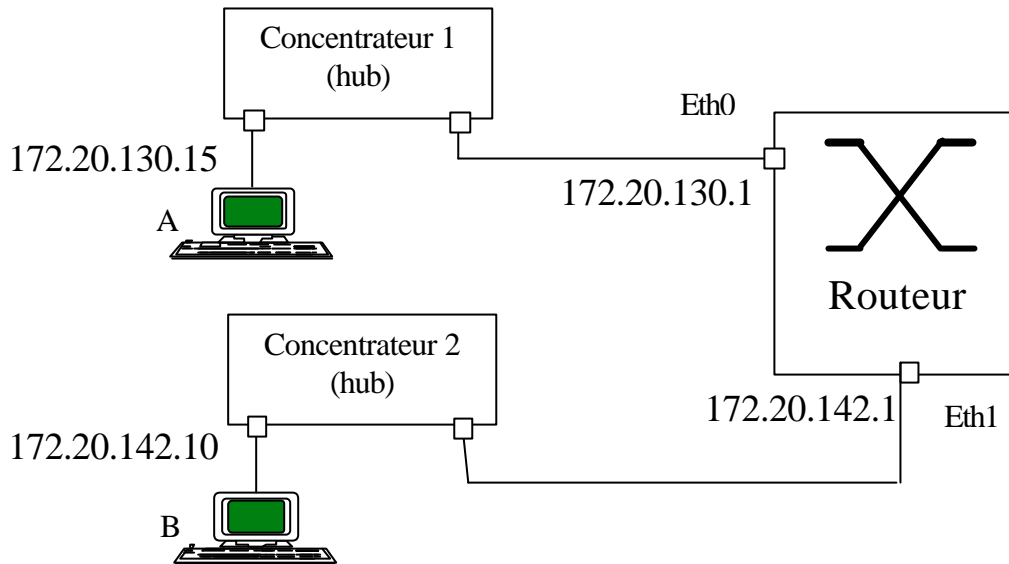
## Question 6

*S'il n'existe plus lors de l'une des étapes précédentes de route possible pour atteindre le destinataire, que se passe t'il?*



## Exercice 3 : Analyse d'un routage IP V4

Pour une expérimentation on a construit un réseau très simple en utilisant le bloc d'adresses IPV4 172.20.0.0/16. Dans la configuration, on a un routeur qui relie deux tronçons Ethernet au moyen de deux ports notés sur la figure eth0 et eth1. Une station de travail A, connectée au tronçon eth0 a pour sa carte réseau, l'adresse 172.20.130.15. L'autre station B, connectée au tronçon eth1, a l'adresse 172.20.142.10. On a défini pour les deux sous réseaux (les machines connectées au concentrateur 1 comme A et au concentrateur 2 comme B) le même masque 255.255.128.0.0.



### Question 1

*On a vu en cours, quatre versions successives de l'adressage IP. Dans cette architecture on dit que l'on fonctionne dans le mode d'adressage IP par sous réseaux (IP subnetting). Pourquoi ?*

### Question 2

*Quelle est la table de routage de la station A ?*

### Question 3

*L'utilisateur de la station A émet un message vers B en utilisant sa table de routage. Expliquez ce qui se passe (le message peut-il atteindre la station B) ?*

### Question 4

*Proposez une modification de l'adressage qui améliore le fonctionnement par changement de la valeur du masque unique utilisé (sans changement des adresses). Vous proposerez la valeur de masque qui autorise la taille la plus grande pour les deux sous réseaux.*

## Exercice 5 : Etude d'une table de routage IP V4

Vous avez à travailler sur un réseau IP d'entreprise. Vous devez en comprendre l'architecture. Vous commencez par un premier routeur IP. Vous listez la table de routage de ce routeur qui vous donne différentes informations dont les principales sont rassemblées dans la table suivante. En fonction de la marque d'un routeur, la présentation des informations de routage est légèrement variable mais les informations essentielles sont toujours à peu près les mêmes. On trouve dans la liste suivante associée au type de routeur analysé :

- une destination à atteindre,
- un masque du réseau destination (qui est ici donné en notation habituelle des adresses IP soit la notation décimale pointée),
- le prochain saut soit la prochaine adresse IP à atteindre sur la route,
- le port qui définit l'interface physique du routeur sur laquelle il faut envoyer un datagramme,
- la métrique qui définit le coût de la route jusqu'au destinataire,
- le type de la route qui est soit directe (DIR), c'est-à-dire que l'on peut délivrer au destinataire final, soit distante (REM pour remote), c'est-à-dire que l'on doit encore traverser un ou des routeurs.

<i>Destination</i>	<i>Route mask</i>	<i>Next hop</i>	<i>Port</i>	<i>Metric</i>	<i>Type</i>
0.0.0.0	0.0.0.0	172.16.3.65	J3	1	REM
172.16.3.0	255.255.255.192	172.16.3.1	J5	0	DIR
172.16.3.64	255.255.255.192	172.16.3.1	J3	0	DIR
172.16.3.128	255.255.255.192	172.16.3.190	J1	0	DIR
172.16.3.192	255.255.255.192	172.16.3.254	J1	0	DIR
172.16.4.0	255.255.255.192	172.16.3.4	J5	115	REM
172.16.4.64	255.255.255.192	172.16.3.4	J5	90	REM
172.16.4.128	255.255.255.192	172.16.3.4	J5	100	REM
172.16.6.64	255.255.255.192	172.16.3.65	J3	376	REM
172.16.8.0	255.255.255.192	172.16.3.65	J3	90	REM
172.16.8.64	255.255.255.192	172.16.3.65	J3	130	REM
172.16.8.128	255.255.255.192	172.16.3.65	J3	75	REM
172.16.25.0	255.255.255.192	172.16.3.62	J5	30	REM
172.16.25.128	255.255.255.192	172.16.3.62	J5	35	REM
172.16.25.192	255.255.255.192	172.16.3.62	J5	35	REM

### Question 1

*Pour comprendre l'architecture de ce réseau IP vous commencez par vous demander à quels routeurs IP ce routeur est connecté. Comment allez vous procéder vous pour connaître ces routeurs. Dans le cas de la table de routage précédente, listez ces routeurs en donnant pour chacun la caractéristique principale pouvant être déduite des informations que vous possédez (l'adresse IP d'une de ses interfaces)?*

## **Question 2**

*Vous souhaitez ensuite déterminer la liste des sous réseaux IP qui sont immédiatement connectés au routeur que vous étudiez. Comment procédez vous ? Dans l'exemple de la table routage précédente quels sont ces réseaux et quelle est leur taille ?*

## **Question 3**

*En regardant plus en détail la table de routage pour ce qui concerne les routes pour les réseaux immédiatement connectés au routeur, vous remarquez que la colonne prochain saut ('next hop') est renseignée. En cherchant à comprendre la signification de ces informations vous constatez qu'il y a une incohérence et donc une erreur dans l'une de ces routes. Où se trouve l'incohérence ?*

## **Question 4**

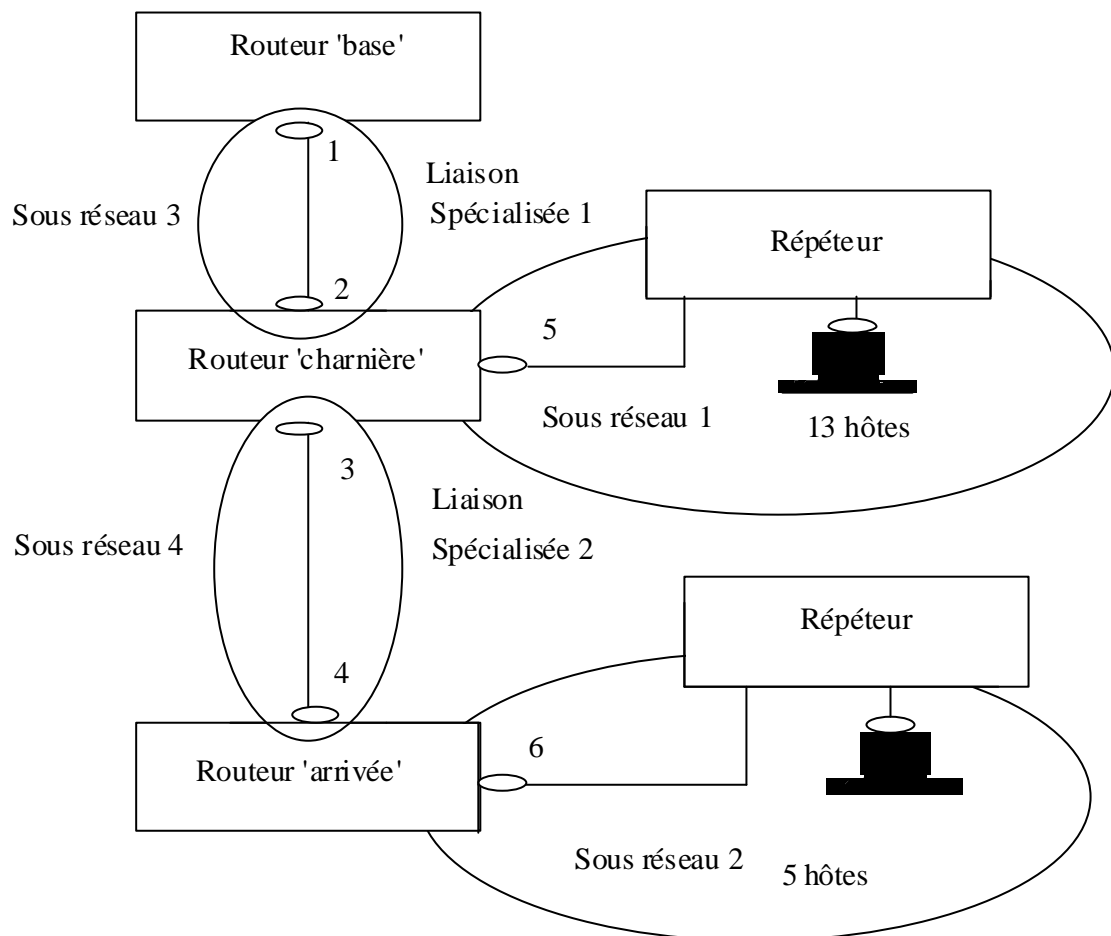
*Pour les routes évoquées à la question précédente (les routes vers les réseaux immédiatement connectés à un routeur), quelle est la signification des informations portées dans la colonne prochain saut ('next hop') de la liste de table de routage ? Que devrait-on faire pour corriger la table de routage ?*

## **Question 5**

*Quelles pouvaient être les conséquences de l'erreur dans la table de routage (quel est le niveau de gravité de cette erreur) ?*

# 10• Déploiement de réseaux IP

Un ingénieur réseau doit installer un nouveau sous-réseau Internet dans son entreprise. L'organisation administrative et géographique des ordinateurs à raccorder est telle qu'il apparaît naturel de créer deux groupes de 5 et 13 hôtes. Chaque groupe de postes est interconnecté au moyen d'un réseau ethernet partagé. On utilise pour cela un répéteur (par exemple de standard 10 BaseT). On associe aux deux groupes, deux sous-réseaux IP et on interconnecte les deux sous-réseaux au moyen de routeurs. Un routeur existant dans l'entreprise baptisé dans la figure suivante routeur 'base' sert à connecter le nouvel ensemble au reste du réseau d'entreprise. Chaque sous-réseau dispose d'un routeur. Ces routeurs sont baptisés 'charnière' pour le groupe de 13 hôtes et 'arrivée' pour le groupe de 5 hôtes. Les routeurs sont connectés au moyen de deux liaisons spécialisées point à point notées Liaison spécialisée 1 et 2.



## Exercice 1 : Choix des adresses

Pour réaliser l'installation IP de ce nouvel ensemble, l'ingénieur réseau souhaite d'une part économiser les adresses IP mais aussi minimiser le nombre des entrées à placer dans les tables de routage pour atteindre le nouvel ensemble (agréger les routes). Pour cela l'ingénieur considère comme indispensable que le nouvel ensemble à installer forme un unique réseau IP, comprenant différentes adresses elles-mêmes organisées en sous réseaux (selon la figure).

Détaillons maintenant toutes les adresses à fournir. Sur le dessin les points qui doivent recevoir une adresse IP sont marqués par de petits ovales.

L'ingénieur réseau doit attribuer des adresses IP pour le sous-réseau 1, c'est à dire pour chacun des 13 hôtes qui constituent ce sous réseau IP, mais aussi pour le port du routeur 'charnière' qui dessert le sous-réseau 1. Ce port est indiqué par le numéro 5 sur la figure.

De même le sous réseau 2 doit comprendre 5 adresses d'hôtes et une adresse pour le port d'accès à partir du routeur 'arrivée'. Ce port est indiqué par le numéro 6 sur la figure.

Les routeurs utilisés ne gèrent pas les liaisons dénumérotées. On rappelle que de nombreux routeurs en appliquant la RFC 1812 permettent d'utiliser des liaisons spécialisées (LS) sans adresses IP. Dans ce cas, moyennant des directives de configuration des routeurs, deux routeurs reliés par une liaison spécialisée forment en fait du point de vue du routage un seul routeur virtuel. La liaison spécialisée est cachée et gérée par le logiciel du routeur. Dans l'exemple traité ici, selon les principes de base de l'adressage IP, il faut attribuer des adresses IP aux deux extrémités d'une liaison spécialisée pour pouvoir l'utiliser dans le cadre du routage. Ces adresses doivent appartenir au même sous réseau IP. Les deux LS forment donc deux petits sous réseaux baptisés 3 et 4. Ces deux sous réseaux ont besoin seulement de deux adresses IP.

L'ingénieur réseau a un bloc d'adresses IP non utilisées dans le cadre d'un adressage de type IPV4 CIDR à partir de l'adresse 193.137.1.0.

### Question 1

Pour le nouvel ensemble l'ingénieur pense pouvoir utiliser seulement un bloc de 32 adresses libres parmi celles dont ils dispose.

*Pourquoi ?*

*Quelle adresse de réseau choisit-il pour la totalité des adresses du nouvel ensemble (donner l'adresse de réseau et son masque en notation /n)?*

### Question 2

L'ingénieur attribue pour commencer les adresses d'extrémité de la liaison spécialisée 1 (adresses du sous-réseau 3). Il doit donc créer un sous réseau avec deux adresses IPV4.

*Quelle est l'adresse de réseau du sous-réseau 3 (l'adresse et le masque du plus petit réseau IPV4 possédant au moins deux adresses utilisables à partir de la première adresse libre) ?*

### Question 3

L'ingénieur attribue la première adresse IP utilisable du réseau déterminé à la question 2 (la plus petite) à l'extrémité 1 sur le dessin (port du routeur 'base') et la seconde (la plus grande) à l'extrémité 2 (port du routeur 'charnière').

*Quelles sont les deux adresses attribuées ?*

### Question 4

L'ingénieur attribue ensuite les adresses IP d'extrémités de la liaison spécialisée 2 (adresses IP du sous réseau 4).

*Quelle est l'adresse de réseau retenue pour ce nouveau bloc de deux adresses si l'on attribue les adresses immédiatement disponibles après l'attribution du sous réseau 3 ?*

### Question 5

*Si l'on attribue la plus petite adresse utilisable de ce sous réseau à l'extrémité 3 (port du routeur 'charnière') et la plus grande adresse à l'extrémité 4 (port du routeur 'arrivée'), quelles sont les deux adresses retenues ?*

### Question 6

L'ingénieur doit ensuite attribuer des adresses de sous réseaux pour les sous réseaux 1 et 2 qui correspondent à 13+1 soit 14 adresses et 5+1 soient 6 adresses.

*Quelle est maintenant la première adresse disponible ?*

*De manière à optimiser l'utilisation des adresses dans quel ordre doit-il attribuer les deux demandes ?*

### Question 7

*Quelle est alors l'adresse de sous réseau attribuée pour le sous réseau 1.*

*Si l'on prend la plus petite adresse disponible dans ce sous réseau, quelle est l'adresse attribuée au port du routeur 'charnière' indiquée 5 sur le dessin ?*

### Question 8

*Quelle est l'adresse de sous réseau attribuée pour le sous réseau 2 ?*

*Si l'on prend la plus petite adresse disponible dans ce sous réseau, quelle est l'adresse attribuée au port du routeur 'arrivée' indiquée 6 sur le dessin ?*

## Exercice 2 : Construction de tables de routage statiques

Dans les questions qui suivent on s'intéresse à la construction des routes dans le cadre d'un routage statique (d'initialisation des tables de routage) pour atteindre les différentes composantes du nouvel ensemble (réseaux, stations, liaisons spécialisées). Pour construire le routage, il peut être très pratique de reporter toutes les adresses définies dans le premier exercice sur la figure qui représente la topologie du réseau pour avoir une vue d'ensemble du plan d'adressage.

### Question 1

Dans la table de routage d'un hôte d'un réseau IP on définit en général trois routes.

*Définir les trois entrées nécessaires au routage pour l'une des stations du sous réseau 1.*

Pour chaque entrée on définira au moins la destination de la route, le masque de cette destination (en notation /n) et le prochain saut ('next hop' ou 'gateway' définissant le prochain routeur ou la station visité).

### Question 2

*Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'base'.*

Pour chaque route on précisera la destination, le masque de la destination, le prochain saut ('next hop' ou 'gateway' définissant le prochain routeur ou la station visité) et le type de la route. Le type est soit local s

les paquets sont délivrés à leur destinataire directement, soit distant si les paquets doivent être relayés par le prochain routeur avant d'être délivré. Pour construire la réponse, on doit définir d'abord la route pour atteindre tout le nouvel ensemble à partir du routeur 'base'. On définira aussi une route qui dessert localement la liaison spécialisée numéro 1. Comme on a créé ce sous réseau IP numéro 1, l'accès à ces adresses doit être possible à toutes fins utiles comme l'envoi de paquets de tests ou de paquets d'administration de réseau SNMP (IP ne sert pas uniquement pour délivrer des messages TCP ou UDP à des hôtes). Cet accès est-il à réaliser par le routeur 'base' via le port numéroté 1?

### **Question 3**

*Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'charnière'.*

Pour chaque route on précisera comme précédemment la destination, le masque de la destination, le prochain routeur et le type de la route (ne pas oublier les liaisons spécialisées).

### **Question 4**

*Définir les entrées concernant le nouvel ensemble, pour la table de routage du routeur 'arrivée'.*

### **Question 5**

*Est ce que le plan d'adressage précédent est satisfaisant ?*

On examinera le critère de l'utilisation des adresses IP. On examinera ensuite le critère de l'agrégation des routes (de la minimisation du nombre de routes à créer).

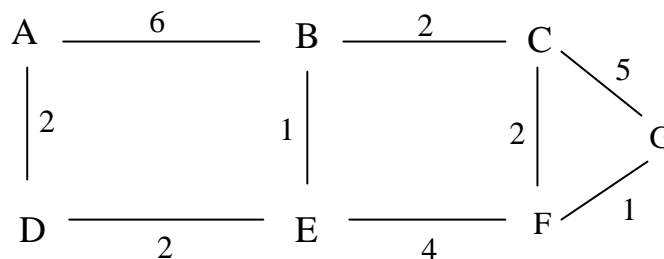
*De combien d'entrées a-t-on besoin dans une table de routage pour accéder au nouvel ensemble des deux sous réseaux ou à chacun des sous réseaux ?*

# 11•Routage OSPF

## ("Open Shortest Path First")

Le but de ce problème est d'étudier le protocole internet OSPF. C'est un protocole de routage réparti dans lequel chaque routeur gère une base de données de l'ensemble des liaisons d'un réseau (topologie du réseau) et calcule à partir de cette base les plus courts chemins par l'algorithme de Dijkstra. Cette base de donnée est mise à jour par diffusion en inondation par chaque routeur de l'état de ses liaisons aux autres routeurs. Il entre dans la classe des protocoles baptisés "à état des liaisons" ou "linkstate".

Par exemple soit un réseau de 7 routeurs A, B, C, D, E, F, G dont la topologie est la suivante (les coûts de transit pour chaque liaison sont supposés égaux dans chaque direction et sont mentionnés sur l'arc représentant la liaison).



La base de données (topologie ou carte du réseau) qui doit être connue de chaque routeur donne principalement les coûts en point à point pour chaque liaison. D'autres informations sont également stockées dans cette table. Certaines de ces informations seront introduites dans la suite.

La base de données (topologie ou carte du réseau) qui doit être connue de chaque routeur donne principalement les coûts en point à point pour chaque liaison. D'autres informations sont également stockées dans cette table. Certaines de ces informations seront introduites dans la suite.

De	Vers	Coût
A	B	6
A	D	2
B	A	6
B	C	2
B	E	1
C	B	2
C	F	2
C	G	5
D	A	2
D	E	2
E	B	1
E	D	2
E	F	4
F	C	2
F	E	4
F	G	1
G	C	5
G	F	1



Cette base de données est construite par échange d'informations entre les routeurs. Pour cela le protocole suivant est effectué. Son déclenchement peut répondre à différentes stratégies de mise à jour :

- périodiquement
- lorsqu'un routeur nouveau s'initialise
- lorsqu'un routeur s'aperçoit qu'il a un nouveau voisin
- lorsque le coût d'une liaison avec un voisin a changé

• Étape 1 :

Chaque routeur construit un paquet appelé "paquet d'état des liaisons" ou LSP ("Link State Packet") qui contient des coûts de liaison que le routeur souhaite faire connaître. Un LSP comporte principalement une liste de noms de routeurs (voisins d'un routeur) et les coûts pour les atteindre. Les LSP émis par un même routeur sont numérotés au moyen d'un numéro de séquence. Pour simplifier on ne se préoccupe pas du retour à zéro des compteurs utilisés trop longtemps.

• Étape 2 :

Le paquet LSP est transmis à tous les routeurs voisins et chaque routeur enregistre les informations du LSP généré le plus récemment. Plus précisément chaque voisin effectue le traitement suivant:

- Recevoir le paquet LSP.
- Consulter la base existante.
- Si l'entrée (la liaison et son coût) n'est pas présente, ajouter cette entrée et diffuser l'information à tous les voisins sauf l'émetteur du LSP.
- Si l'entrée est présente et si le numéro de séquence du LSP est plus grand que celui correspondant à l'entrée modifier l'entrée et diffuser l'information à tous les voisins sauf le ré-émetteur du LSP.
- Si l'entrée est présente et si le numéro de séquence du LSP est plus petit ou égal à celui correspondant à l'entrée: ne rien faire.

## Question 1

Les protocoles de routage de type vecteurs de distance dont l'exemple type est le protocole Internet RIP ("Routing Information Protocol") se distinguent des protocoles de type Internet OSPF (à état de liaison).

*Rappeler en quelques lignes l'algorithme que doit suivre chaque routeur pour le protocole RIP.*

## Question 2

*A quoi pourrait servir la retransmission du LSP à son émetteur ?*

*Pourquoi un paquet LSP n'est-il pas renvoyé à son émetteur ?*

## Question 3

*A quoi sert le Numéro de Séquence émetteur du point de vue du réseau internet qui est à datagramme ?*

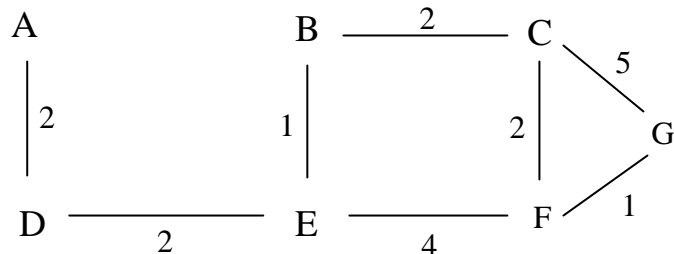
*A quoi sert le Numéro de Séquence émetteur du point de vue du protocole de diffusion des informations d'état de liaison ?*

En plus du Numéro de Séquence, chaque information concernant une liaison possède une date de péremption (variable baptisée dans OSPF "age") qui apparaît aussi bien dans les paquets LSP échangés que dans les bases de données. Toute information dépassant sa date est systématiquement détruite.

*Citer plusieurs types de problèmes qu'une telle datation solutionne.*

#### Question 4

On suppose que la liaison de A vers B est coupée. On a alors le réseau :



A ayant détecté la coupure, A prépare un LSP de la forme : "de A à B, coût = infini , numéro de séquence,"

On suppose que ce LSP est le premier généré (au début il est le seul).

*Indiquer ce qui se passe alors dans le réseau. Quelle est la base de données obtenue par les différents noeuds à la fin du processus d'inondation ?*

On suppose qu'ensuite B prépare et transmet son LSP concernant A-B.

*Quelle est la base de données obtenue ?*

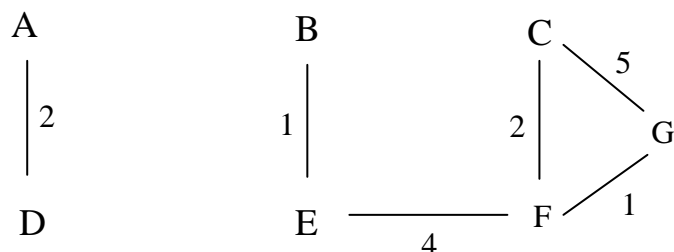
#### Question 5

On suppose que la liaison de D à E tombe en panne (on suppose que les 2 noeuds D et E se sont aperçus de cette rupture et envoient les LSP correspondants).

*Indiquer la (ou les) bases de données obtenues à l'issue de l'algorithme distribué de transmission de l'état des liaisons par chacun des noeuds.*

#### Question 6

A partir des bases de données trouvées à la question précédente et du réseau suivant on suppose que la liaison de B à C tombe en panne et amène au réseau :

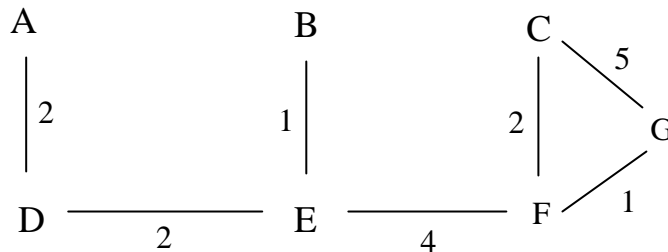


*Indiquer les bases de données obtenues par chaque routeur.*

## Question 7

Par la suite la liaison de D à E est rétablie avec un coût de 2 rendant de nouveau le réseau connexe. On obtient alors le réseau ci-dessous.

On exécute l'algorithme de diffusion en supposant que D et E informent le réseau du rétablissement de cette connexion.



*Quelle est la valeur du coût de la liaison de B à C pour les sites A, D et pour les sites B, C, E, F ?*

*Quel est le risque encouru dans cette situation ?*

*Comment détecter efficacement la situation ? Sur quel type de site ? (on suggère une utilisation du numéro de séquence)*

*Comment faire pour mettre en oeuvre une solution de "réconciliation" basée sur le numéro de séquence ?*

## Question 8

*La technique de diffusion par inondation de l'état des liaisons est inconcevable telle que pour le réseau Internet. Pourquoi ?*

*Que fait-on pour appliquer quand même OSPF à l'internet ?*

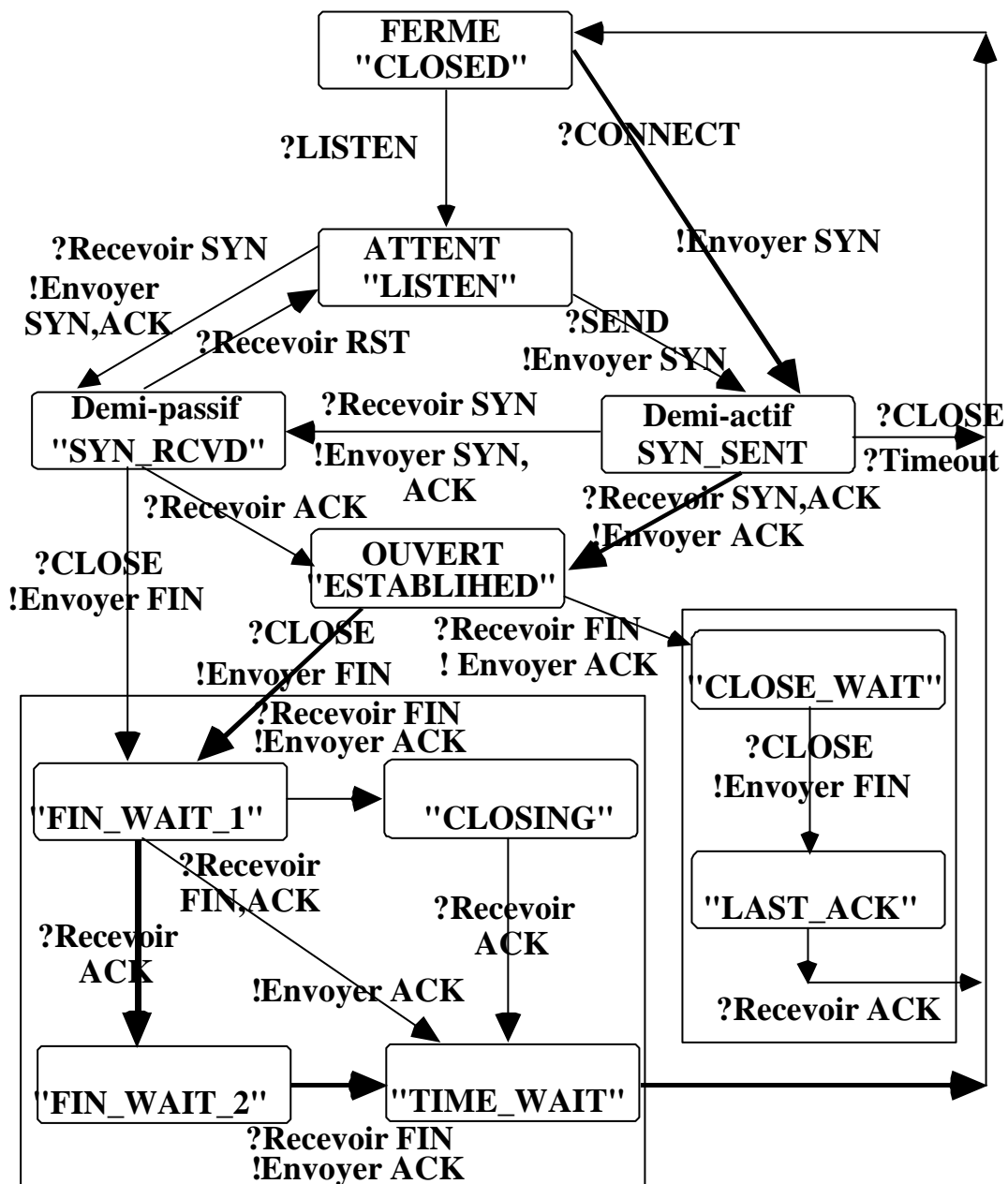
# 12• TCP : automate protocolaire

Citez différentes raisons qui justifient l'introduction de la couche transport dans la pile des protocoles de communication OSI.

Rappelez les principaux choix de conception du protocole de transport TCP.(quelles sont les fonctions réalisées par TCP?).

Examinez l'automate en suivant les transitions portées en traits gras. Il s'agit d'une ouverture de connexion suivie d'une fermeture. Analysez les différentes étapes d'une ouverture de connexion entre un client et un serveur.

Que se passe-t-il lors de la fermeture de connexion?



# 13• TCP : fonctionnement

## Exercice 1 : Généralités sur la couche transport

### Question 1

*Quels sont les problèmes posés par l'utilisation de couches réseaux peu fiables qui compliquent la réalisation de la couche transport ?*

### Question 2

*Quelles sont les principales analogies entre la couche transport et la couche liaison ?*

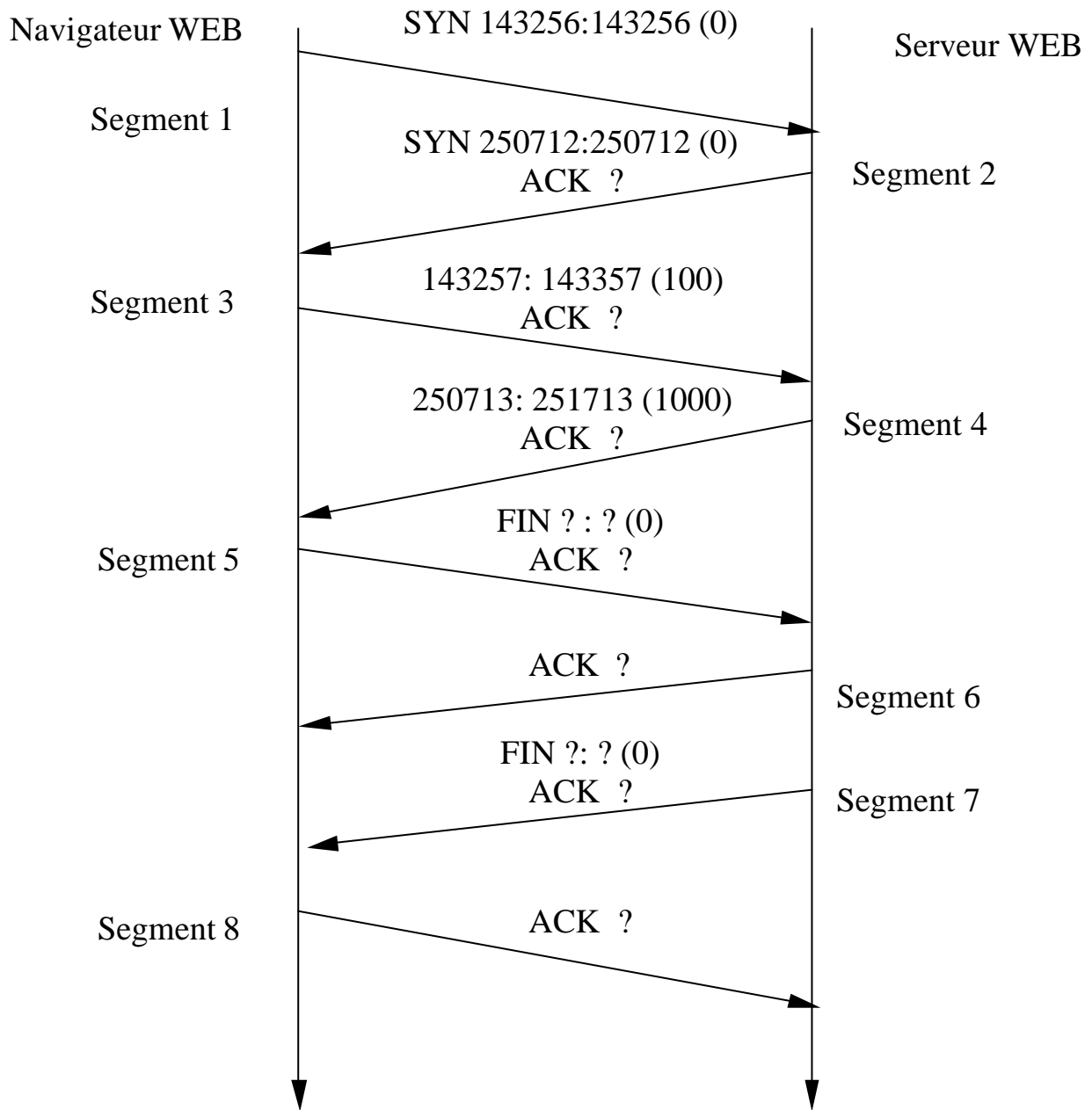
*Quelles en sont les principales différences ?*

## Exercice 2 : Transport TCP

L'échange TCP de la figure suivante 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 1000 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 à côté 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.*



## Exercice 2 : TCP, Evolutions et Approches alternatives

### Question 1

*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).*

### Question 2

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

*2.2. Rappelez brièvement les principes des mécanismes baptisés "slow-start", et "congestion avoidance" du protocole TCP. Eventuellement, aidez-vous d'un dessin et indiquez sur ce dessin la partie correspondant au "slow-start" et la partie correspondant à "congestion avoidance".*

### Question 3

TCP a une approche réactive pour estimer la bande passante disponible pour une connexion. En fait, le débit soumis augmente tant qu'une congestion n'apparaît pas (et tant qu'on ne dépasse pas le crédit alloué par le récepteur). Différentes études proposent des modifications de TCP.

TCP se voit ajouter des extensions. On examine une extension qui est relative au débit d'émission. Des statistiques sont faites par connexion.

- On calcule un débit attendu instantané de la façon suivante :

$$\text{Attendu}(t) = \text{TailleFenêtreCongestion}(t) / \text{BaseRTT} \text{ où}$$

- BaseRTT : délai Aller/Retour associé à un segment quand le réseau n'est pas congestionné (avant que les routeurs ne saturent à cause du trafic de cette connexion), on entend par délai Aller/retour (ou encore RTT pour Round Trip Time) le délai qui s'écoule entre l'émission du segment et l'arrivée de son acquittement. BaseRTT est le plus petit RTT mesuré. Il est mesuré à chaque fois qu'on émet un segment, si lors du retour de l'acquittement du segment, le RTT associé à celui-ci est inférieur à BaseRTT, alors BaseRTT prend cette nouvelle valeur.
- TailleFenêtreCongestion(t) est la valeur courante de la fenêtre de congestion de l'émetteur.

- On mesure le débit d'émission réel instantané de la façon suivante :

$$\text{Mesuré}(t) = \text{TailleSegmentEmis}(t) / \text{RTTduSegment}$$

Soit  $\text{Diff}(t) = \text{Attendu}(t) - \text{Mesuré}(t)$

*3.1. Expliquer pourquoi  $\text{Diff}(t)$  ne peut être négatif.*

Deux seuils sont définis :  $A < B$

Si  $\text{Diff}(t) < A$  alors la fenêtre de congestion augmente linéairement.

Si  $A < \text{Diff}(t) < B$  alors rien n'est fait.

Si  $B < \text{Diff}(t)$  alors la fenêtre de congestion diminue linéairement.

3.2. *A quoi correspondent les seuils A et B ?*

3.3. *Expliquer en quoi, cette modification vous semble permettre d'augmenter l'efficacité de TCP vis-à-vis de l'occurrence des congestions.*

#### **Questions 4 : UDP et gestion de la congestion dans Internet.**

4.1 *Quel type de mécanisme faudrait-il ajouter dans le protocole UDP ou en dehors du protocole UDP pour qu'il ne contribue pas à la saturation d'Internet quand un utilisateur tente d'émettre à un fort débit indépendamment de la charge du réseau.*

4.2 *Comment devrait alors se comporter une relation ou une "connexion" de cette nouvelle version d'UDP du point de vue du partage de la bande passante de l'Internet vis-à-vis des connexions TCP co-existant sur le réseau ? La réponse doit uniquement considérer le point de vue de la couche transport. Il faut donc imaginer que le comportement au niveau transport est indépendant d'un mécanisme de réservation de ressources tel que RSVP, cela doit fonctionner même sur un réseau de type best effort.*



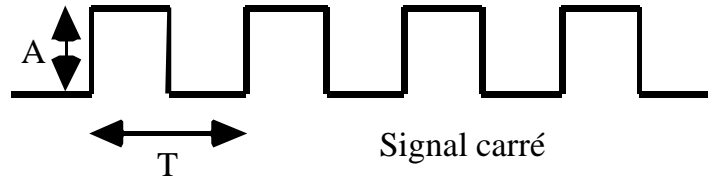
# **Annexe :**

# **Compléments d'exercices**

# Théorie du Signal

## Exercice : Densité spectrale de signaux binaires simples

Nous nous intéressons à un signal carré d'amplitude  $A$  et de période  $T$ .



### Question 1

*Rappeler comment le signal représenté dans la figure ci-dessus se décompose en une somme de signaux élémentaires (harmoniques).*

Pour cela, on rappellera le résultat du développement en série de Fourier de ce signal sachant que la fonction qui le représente est périodique et qu'on peut la considérer comme une fonction paire.

### Question 2

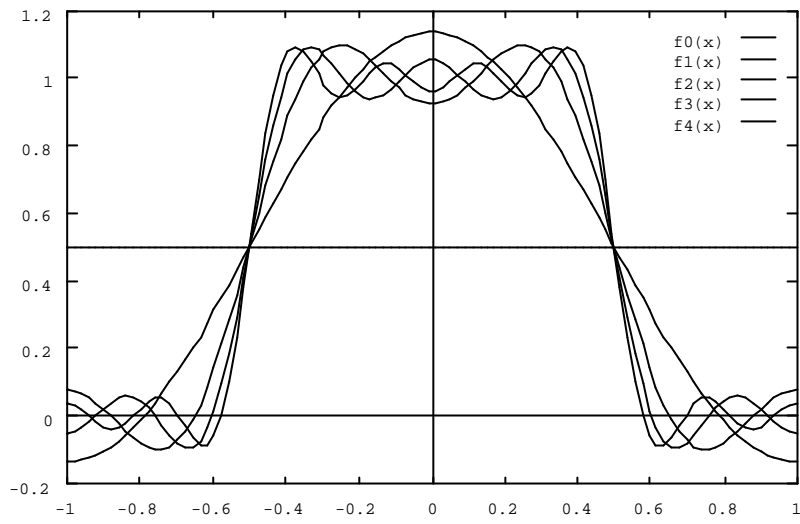
*Déterminer la puissance contenue dans les différentes harmoniques.*

*En déduire la largeur de bande d'un filtre qui laisse passer 90 %, puis 98 % de la puissance contenue dans le train d'impulsions.*

*Faire une application numérique pour une transmission à 200 bauds.*

A titre indicatif, voici le tracé de la superposition des premières harmoniques du signal carré, calculé avec le logiciel GNUplot :

```
gnuplot> f0(x)=0.5
gnuplot> f1(x)=f0(x)+2*sin(pi/2)/pi*cos(pi*x)
gnuplot> f2(x)=f1(x)+2*sin(3*pi/2)/pi/3*cos(3*pi*x)
gnuplot> f3(x)=f2(x)+2*sin(5*pi/2)/pi/5*cos(5*pi*x)
gnuplot> f4(x)=f3(x)+2*sin(7*pi/2)/pi/7*cos(7*pi*x)
gnuplot> plot f0(x),f1(x),f2(x),f3(x),f4(x)
```



# Commutation & Multiplexage

## Exercice 1 : Commutation

On rappelle que la modulation MIC est destinée à numériser la transmission de voix téléphoniques. L'intervalle de temps séparant la prise de deux échantillons d'une même voix est de 125  $\mu$ s. Le signal analogique est échantillonné sur 8 bits.

### Question 1

*Quel est le débit utilisé pour transmettre une voix téléphonique ?*

Ces paramètres d'échantillonnage résultent de la bande passante offerte par une ligne téléphonique.

*Quelle est la largeur de bande considérée dans le MIC ?*

*Quelles relations lient la largeur de bande, le débit et les paramètres d'échantillonnage ?*

### Question 2

La principale technique de commutation utilisée sur les autocommutateurs téléphoniques numériques (associée à la modulation MIC) est la commutation temporelle synchrone.

*A quoi sert un autocommutateur ?*

*Expliquer en quelques lignes les principes de la commutation temporelle synchrone.*

### Question 3

Un commutateur gère N lignes en entrée et N lignes en sortie. On considère pour simplifier que toutes les lignes ont le même débit et qu'aucun multiplexage temporel n'est réalisé. Le commutateur utilise une mémoire dont le temps de lecture ou d'écriture est de 50ns (ce temps correspond à une lecture ou à une écriture entre les interfaces de lignes et la mémoire).

Le pseudo-code suivant décrit le processus de commutation, à l'exception de l'affectation des lignes d'entrée aux lignes de sortie.

```
Processus commutateur  
type num_ligne: entiers dans [1..N];  
  
var échantillon: tableau (1..N) d'octets;  
    ligne_sortie: tableau (1..N) de num_ligne;  
    i:num_ligne;  
début  
    cycle  
        pour i:=1 à N faire  
            attendre_top;  
            lire(i,échantillon(i));  
            écrire(ligne_sortie(i);échantillon(i));  
        finpour  
    fincycle  
fin
```

*Quel est l'usage du tableau `ligne_sortie` ?*

*Que font les opérations `lire` et `écrire` ?*

*A quoi sert l'instruction `attendre_top` ?*

On suppose que les instructions `lire` et `écrire` prennent un accès mémoire et que le temps d'accès à l'index et que le temps de gestion de la boucle sont négligeables (l'implantation réelle est cablée).

*Quelle est la valeur maximale de  $N$  (justifier) ?*

Soit  $T$  le temps séparant l'apparition de deux événements `attendre_top`.

*Si  $N=600$  quelle valeur doit-on donner à  $T$  (justifier) ?*

#### **Question 4**

On considère que le même problème de commutation (sans multiplexage) doit être résolu en utilisant la commutation de cellules. Chaque cellule correspond à un échantillon.

*Rappeler brièvement les principes de la commutation de cellules.*

*Comment les structures d'informations définies dans la question 3 doivent-elles être modifiées pour faire de la commutation de cellules (on ne traitera pas le problème de la gestion de la table de routage).*

*Réécrire le pseudo-code du commutateur de paquets.*

On souhaite en utilisant les principes de la commutation de paquets en mode datagramme transmettre des informations de type voix, images télévisées numérisées, données, etc. à très haut débit (1 à 5 gigabit/s).

*Quels sont les principaux problèmes techniques que cela pose ?*

## **Exercice 2 : Multiplex T1**

Aux États unis et au Japon les réseaux téléphoniques utilisent un multiplexage baptisé T1 de 24 octets formant une trame de base (trame du multiplex T1). Il existe différentes versions du codage T1. Nous considérons ici le cas où les 24 octets sont associés à des échantillons de voies téléphoniques.

#### **Question 1**

Dans une trame T1, aux échantillons téléphoniques, est ajouté un bit placé en tête qui sert à la resynchronisation trame en cas de perte de synchronisation (bruit de longue durée).

*Quel est le débit binaire global d'un multiplex T1 ?*

#### **Question 2**

On considère un commutateur temporel synchrone de multiplex T1 à mémoire commune dont le temps d'accès est de 20 ns — c'est à dire que pour accéder à un échantillon en mémoire, en lecture comme en écriture, il faut 20 ns.

*Combien de multiplex T1 un tel commutateur temporel synchrone peut-il supporter au maximum ?*

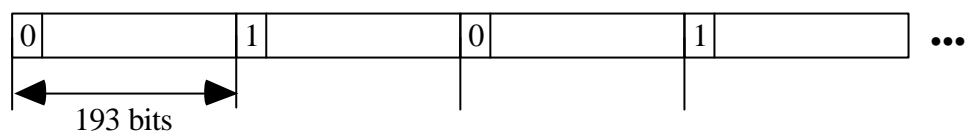
#### **Question 3**

Un échantillon est commuté d'un multiplex d'entrée du commutateur vers un multiplex de sortie du commutateur en un certain délai.

*Que peut-on dire de la valeur maximum, minimum, moyenne du délai nécessaire à une opération de commutation (retard apporté dans la propagation de l'échantillon sur un circuit téléphonique par un commutateur) ?*

#### Question 4

On rappelle que le premier bit est rajouté pour la synchronisation trame. La synchronisation est trouvée lorsque le premier bit de trames successives respecte la séquence 0, 1, 0, 1, 0... Plus précisément la suite des trames est :



Pour être synchronisé, il faut donc constater tous les 193 bits l'alternance 0, 1, 0, 1, 0, ... si le premier bit lu a été un 0 ou bien 1, 0, 1, 0, 1, ... si le premier bit lu a été un 1.

On suppose que le multiplexeur cherche à se resynchroniser (par exemple après avoir subi un bruit sur plusieurs trames successives). Pour cela, il se positionne sur un bit qu'il estime être le début de la trame courante et vérifie que 193 bits plus loin, il trouve le bit de début de la trame suivante (de valeur contraire à la valeur précédente). On suppose que les bits 0 et 1 apparaissent avec la même probabilité 1/2 dans les échantillons en n'importe quelle position d'une trame.

*Combien faut-il inspecter de trames pour avoir une probabilité d'erreur de resynchronisation inférieure à 0.001 ?*

#### Question 5

On veut maintenant calculer le nombre de trames qu'il faut inspecter en moyenne pour être sûr que la synchronisation n'est pas correcte. On se positionne sur un bit donné en faisant l'hypothèse que ce bit est le début d'une trame.

Si ce bit n'est pas le bit de début de trame, donnez la probabilité pour apprendre que la resynchronisation n'est pas trouvée en lisant une seule trame, puis en lisant deux trames, puis en lisant n trames (on utilise une partie des calculs de la question précédente).

*En déduire combien il faut inspecter en moyenne de trames successives pour apprendre que la synchronisation n'est pas correcte pour une position donnée.*

On rappelle la formule : pour  $|x| < 1$ ,  $\sum_{n=1}^{+\infty} nx^n = \frac{x}{(1-x)^2}$

# Réseaux locaux sans fils

## IEEE 802.11 WIFI

### Fonctionnement du protocole d'accès au médium

La norme IEEE 802.11 définit un réseau local sur voie hertzienne (réseau local sans fils ou WLAN Wireless LAN). La gamme de débits visée est de 1 Mb/s, 2 Mb/s, 11 Mb/s selon les normes et les bandes de fréquences utilisées. Le protocole d'accès au médium présente des différences significatives avec Ethernet en particulier il existe deux catégories de mode de partage de la voie commune radio utilisée pour communiquer.

#### Question 1

Dans l'une des deux organisations baptisée « ad'hoc », le réseau s'auto-organise en fonction des stations qui se trouvent suffisamment proches et peuvent communiquer par radio. La méthode de partage de la voie commune (méthode d'accès au médium ou encore niveau MAC) utilisée est alors baptisée DCF ("Distributed Coordination Fonction"). Elle est conçue pour des communications asynchrones dans lesquelles chaque station a une chance égale d'accéder au médium. Le partage de la voie commune radio est de type CSMA.

*Que signifie CSMA et quel est le choix technique relativement au protocole d'accès au médium réalisé en adoptant le CSMA ?*

#### Question 2

Le mode d'ajournement utilisé dans le partage de la voie commune radio 802.11 est un ajournement non persistant. Lorsqu'une station souhaite émettre elle écoute la voie. Si pendant un délai fixe baptisé DIFS ("Distributed Inter Frame Spacing") aucune autre station n'émet, la station commence à émettre à l'issue du délai DIFS. Si une station a déjà commencé à émettre, la station en écoute ajourne sa transmission pendant toute la durée du message en cours. A l'issue de cette attente, elle attend en plus un délai initialisé à une valeur calculée selon une méthode analogue à celle du 'binary backoff' d'Ethernet.

*Rappelez le principe d'un ajournement persistant et non persistant.*

#### Question 3

*Pourquoi choisir un ajournement non persistant dans un réseau local sans fil présentant les caractéristiques de 802.11?*

#### Question 4

Lorsqu'une station doit ajourner à plusieurs reprises sa transmission parce que la voie est occupée par d'autres stations, elle laisse passer les autres. A chaque fois, quand la voie est redevenue libre, elle recommence à décrémenter la valeur initialement déterminée par l'algorithme de backoff (sans recalculer une nouvelle valeur du délai selon le backoff).

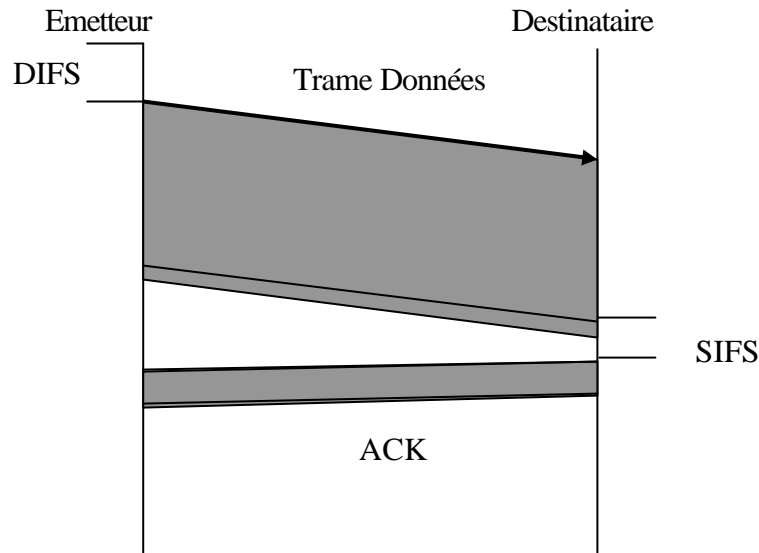
*Lorsque le délai initialement déterminé est écoulé, elle commence à transmettre, pourquoi procéder ainsi (pourquoi ne pas repartir sur une valeur plus longue à chaque ajournement)?*

### Question 5

*Lorsque l'on transmet un message en 802.11 on risque néanmoins une collision, pourquoi ?*

### Question 6

La détection des collisions réalisée par le réseau Ethernet étant coûteuse et inefficace dans le mode des communications radio, le mode de traitement des collisions utilisé est un mode par acquittement positif.



Toute trame de donnée est suivie, après une attente courte baptisée SIFS ('Short Inter Frame Spacing'), d'une trame d'acquiescement positif par le destinataire. Si l'acquiescement positif n'est pas retourné, l'émetteur considère qu'il y a eu collision. Il entre alors dans une phase d'attente aléatoire définie de manière similaire à celle du réseau Ethernet. Les différences portent sur les constantes de temps et d'initialisation de l'algorithme du retard binaire ('binarybackoff').

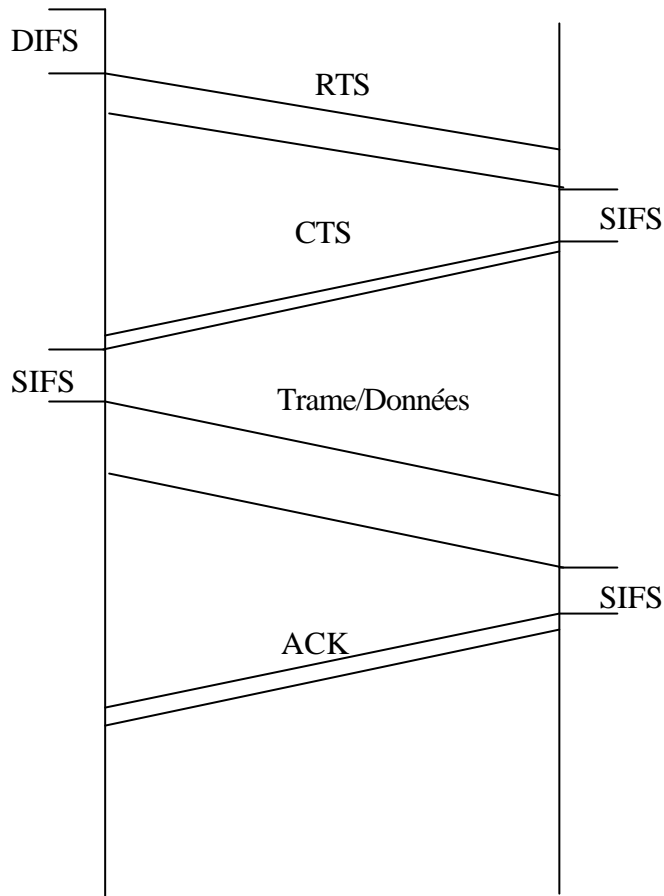
*Pourquoi une telle attente en cas de collision?*

*Comment est calculée la valeur du délai d'attente (backoff) en Ethernet?*

### Question 7

Dans un autre mode de fonctionnement de la méthode d'accès ad'hoc (protocole DCF de la proposition IEEE 802.11), une station émettrice commence par émettre un message court RTS "Request To Send" pour réserver l'intervalle de temps nécessaire à la transmission de son prochain message. Le message RTS contient l'adresse émetteur, l'adresse du destinataire et le temps d'occupation de la bande radio. Le destinataire répond, après un silence inter trame court SIFS, le message CTS "Clear To Send" indiquant qu'il a bien reçu la demande de réservation. Il rappelle les paramètres de la communication à venir dans le message CTS. Toutes les autres stations du réseau entendent également cet échange. Ensuite la trame de donnée et son acquiescement sont échangés comme précédemment. L'ensemble de l'échange est donc le suivant :





Ce protocole d'accès au médium est baptisé par ses auteurs CSMA/CA (CA pour Collision Avoidance).

*Est ce qu'il évite réellement toutes les collisions ? En quoi améliore t'il le traitement des collisions par rapport à la version de base qui pratique l'échange direct d'une trame de donnée suivie de son acquittement ?*

### Question 8

Dans l'autre organisation du réseau baptisée 'infrastructure', le réseau est organisé en cellules appelées BSS ("Basic Service Set"). Chaque cellule réunit plusieurs stations ayant un coupleur IEEE 802.11 et possède un dispositif spécifique baptisé point d'accès AP ("Access Point") qui connaît toutes les stations de la cellule. Dans ce mode, le point d'accès AP joue le rôle d'arbitre centralisé dans un protocole de communication par scrutation (ou 'polling').

*Rappelez les principes généraux d'un protocole de partage d'une voie commune par scrutation ?*

### Question 9

Les concepteurs des réseaux 802.11 ont adopté le mode polling en particulier pour la transmission de données temps réel ou multimédia (comme la voix ou la vidéo) qui demandent un respect de contraintes temporelles assez strictes (exemple respect de l'isochronisme des échanges).

*Rappelez la définition d'une transmission isochrone.*

### **Question 10**

*Pourquoi le mode par scrutation permet t'il d'assurer le respect du temps de réponse ou de la gigue ?*

## **Fragmentation dans les réseaux locaux sans fils WIFI**

Le réseau local 802.11 est un réseau local radio. Dans ce texte on étudie les problèmes liés au bruit dans les transmissions radio et leur liaison avec la fragmentation. On prend l'exemple de la version IEEE 802.11/b à 11 megabits/seconde.

### **Question 1**

*Si la probabilité d'erreur par bit sur une voie de communication utilisée par un réseau local est  $p$ , que les erreurs sont indépendantes et que le nombre de bits d'une trame est  $n$ , quelle est la probabilité d'erreur pour une trame complète ? Dans la suite on note  $q$  cette probabilité.*

*Application numérique : Quelle est la probabilité d'erreur par trame pour  $p=10^{-6}$  et une trame 802.11 de longueur maximum conforme au standard soit 2346 octets ?*

### **Question 2**

*Pour une probabilité d'erreur par trame  $q$ , déterminez le nombre moyen  $E$  de tentatives à réaliser pour réussir une transmission correcte ?*

*On rappelle que  $1/(1-q)^2 = 1+2q +3q^2+ \dots +nq^{n-1} + \dots$  Application numérique : Quel est le nombre moyen de tentatives de transmission d'une trame que l'on doit effectuer pour réussir une transmission correcte pour  $p=10^{-6}$  ?*

### **Question 3**

*On veut faire une première évaluation grossière du débit binaire perdu du fait des retransmissions sur erreur. On ne tient donc pas compte d'aucun autre facteur que les erreurs de transmission. Pour une probabilité d'erreur par trame  $q$ , un débit nominal de transmission  $d$ , quel est le débit utile et quel est le débit consacré aux retransmissions pour une voie qui est utilisée en permanence (il y a toujours une trame à transmettre, la voie est saturée) ?*

*Application numérique : Quel est le débit utile et quel est le débit consacré aux transmissions en erreur pour la norme 802.11/b avec  $d=11$  megabits/s,  $p=10^{-6}$  ?*

#### **Question 4**

En dehors des réseaux locaux sans fils 802.11, il existe de très nombreuses variantes de protocoles de liaison et de protocoles d'accès au médium dans les réseaux locaux.

*Quels sont les mécanismes prévus pour la fragmentation dans les protocoles de liaison (justifiez les choix qui sont faits) ?*

#### **Question 5**

*Les normalisateurs des réseaux sans fils 802.11 ont décidé de prévoir une fonctionnalité de fragmentation. Supposons que l'on fragmente une trame de  $n$  bits en  $k$  fragments et que comme précédemment on ne tient pas compte d'aucun autre facteur que les erreurs de transmission, que devient le débit utile et que devient le débit perdu à effectuer des retransmissions ?*

*Application numérique : Quel est le débit utile et le débit perdu pour une trame de 2346 fragmentée en 4 fragments, pour la probabilité d'erreur par bit de  $10^{-6}$  ?*

#### **Question 6**

En fait, fragmenter en des fragments de plus en plus petit pour améliorer le débit utile n'est pas possible.

*Quels sont les différents facteurs qui limitent l'utilisation de la fragmentation dans les réseaux sans fils 802.11 pour traiter le problème des erreurs ?*

#### **Question 7**

Le fait de déclencher le mécanisme de fragmentation n'est pas défini de façon précise dans la norme 802.11. Il est indiqué qu'une implantation définit un seuil en deçà duquel on ne fait pas de fragmentation et au delà duquel on fragmente.

*Proposez des principes de fixation d'un tel seuil et des principes de choix d'une taille de fragment dans l'implantation d'un coupleur 802.11 ?*

#### **Question 8**

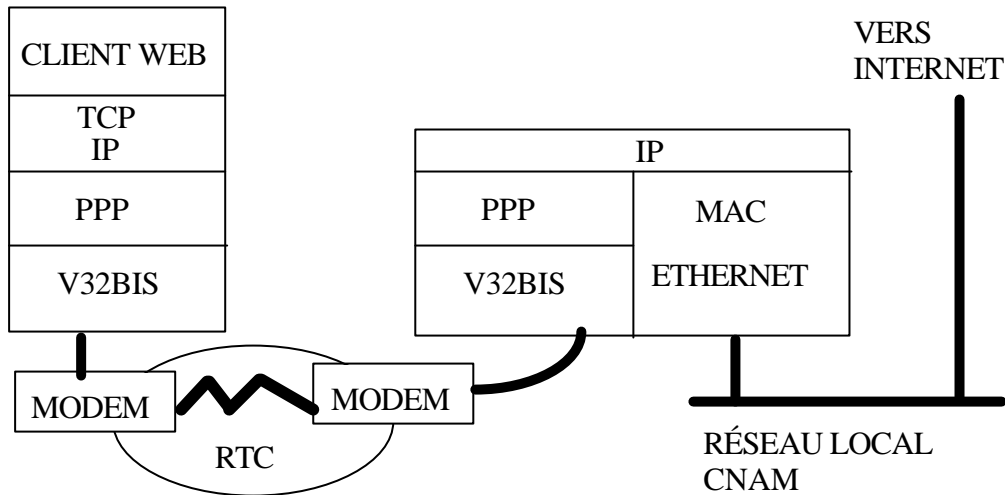
La fragmentation 802.11 est une fragmentation transparente. De plus les fragments en 802.11 sont soumis à un contrôle d'erreur avec retransmission et ils se suivent sur la voie hertzienne (ils ne peuvent être déséquenceés).

*Rappelez les informations nécessaires à la fragmentation IPV4. Proposez une simplification de ces informations qui fonctionne néanmoins dans le cas particulier du réseau sans fil 802.11 ?*

# Dimensionnement et coûts

## Application à un service de dialup IP

Le dialup IP est une technique de connexion à un réseau Internet de manière intermittente via le RTC. Il repose souvent sur le protocole d'échange de trames PPP (Point to Point Protocol).



Le Centre de Ressources Informatique du CNAM utilise cette technique pour offrir à ses usagers un accès distant à l'Internet. Pour ce faire, il a installé un pool de  $N$  modems et loué une ligne groupée à France-Télécom. Il utilise actuellement (mai 98) 10 modems à 14400 bit/s (norme V32) et 15 modems 28800 bit/s (norme V32bis) dont 5 réservés au Centre pour le rétro appel.

On veut étudier dans cet exercice le dimensionnement et le coût (financier) de l'accès vers Internet dans l'hypothèse d'une montée en puissance du service dialup, qui n'est à l'heure actuelle pas offert à tous.

On ne tiendra pas compte dans l'analyse du trafic causé par les autres machines du CNAM !

### Exercice 1 : Dimensionnement du service

On peut assimiler les  $N$  lignes groupées à une file d'attente de capacité  $N$ . Quand toutes les lignes sont occupées, un nouvel appelant trouve les lignes occupées et se voit rejeté. La probabilité de rejet  $P_{rej}$  est fonction :

- du nombre de lignes  $N$
- du temps moyen écoulé entre deux appels successifs, noté  $EA$
- de la durée moyenne des appels, notée  $ES$

Elle se calcule grâce à la formule d'Erlang : 
$$P_{rej} = \frac{r^N / N!}{\sum_{i=1}^N r^i / i!}$$

où  $\rho = ES/EA$  définit la charge du système.

Le nombre moyen de lignes utilisées est par ailleurs  $EN = r(1 - P_{rej})$

Ici, on veut plutôt connaître  $N$  en fonction des autres paramètres. Pour cela, on peut utiliser les abaques

en annexe.

## Question 1 : Charge du système et probabilité de rejet

Le logiciel de connexion PPP tient à jour un fichier de statistiques hebdomadaire, dont voici un extrait portant sur le mois de Novembre 1997 :

```
Sunday 26 Oct 97 at 0 h 7 and Sunday 2 Nov 97 at 23 h 58
(8 d 0 h 50 mn 17 s)
Total connections: 1274
(mean 17 mn 26 s per connection, 6.6 connections per hour)
Total time: 15 d 10 h 14 mn 49 s (191 %)
-----
Monday 3 Nov 97 at 0 h 9 and Monday 10 Nov 97 at 0 h 2
(6 d 23 h 52 mn 50 s)
Total connections: 1817
(mean 15 mn 33 s per connection, 10.8 connections per hour)
Total time: 19 d 15 h 8 mn 17 s (280 %)
-----
Monday 10 Nov 97 at 0 h 7 and Monday 17 Nov 97 at 0 h 2
(6 d 23 h 55 mn 23 s)
Total connections: 1819
(mean 16 mn 12 s per connection, 10.8 connections per hour)
Total time: 20 d 11 h 34 mn 25 s (292 %)
-----
Monday 17 Nov 97 at 0 h 5 and Monday 24 Nov 97 at 0 h 1
(6 d 23 h 55 mn 42 s)
Total connections: 1783
(mean 16 mn 2 s per connection, 10.6 connections per hour)
Total time: 19 d 20 h 53 mn 58 s (283 %)
-----
Monday 24 Nov 97 at 0 h 6 and Sunday 30 Nov 97 at 23 h 59
(6 d 23 h 53 mn 11 s)
Total connections: 2128
(mean 15 mn 42 s per connection, 12.7 connections per hour)
Total time: 23 d 5 h 1 mn 11 s (331 %)
-----
Monday 1 Dec 97 at 0 h 5 and Monday 8 Dec 97 at 0 h 3
(6 d 23 h 57 mn 33 s)
Total connections: 1976
(mean 17 mn 24 s per connection, 11.8 connections per hour)
Total time: 23 d 21 h 24 mn 22 s (341 %)
```

*En déduire la charge moyenne sur la période considérée*

*Avec l'abaque d'Erlang, en déduire la probabilité de rejet*

*Que penser du résultat obtenu ?*

## Question 2 : Trafic de pointe

Une analyse plus fine a permis de remarquer que sur 24 h, la *pointe* du trafic est atteinte en fin de journée. 40% des requêtes se font entre 22h et 24h.

*Quelles sont alors la charge et la probabilité de rejet ?*

### Question 3 : Augmentation du nombre d'utilisateur

Actuellement, il y a environ 8000 comptes utilisateurs au Centre de ressources. On voudrait savoir combien il faudrait de modem si on crée un compte pour chaque inscrit au CNAM (80000 env).

*Calculer la charge moyenne pour 80000 comptes.*

*En déduire la probabilité de rejet si  $N=20$ , puis  $N=40$*

*Que devient cette dernière pendant la pointe de trafic ?*

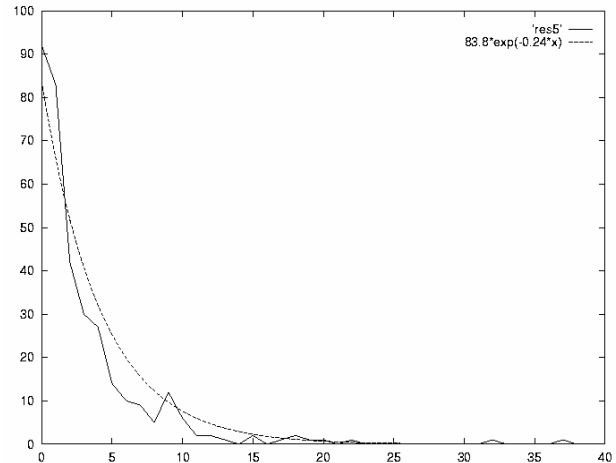
### Question 4 : Débit vers l'extérieur

On suppose que 40 modems à 28800 b/s sont installés.

*Déduire des résultats précédents le débit moyen vers l'extérieur*

#### Remarque

La formule d'Erlang n'est valide que si les temps entre appels successifs sont des variables aléatoire de distribution exponentielle. On le vérifie à peu près ici sur des mesures faites pendant la journée du 9 décembre 1997. Il y a eu ce jour 347 connexions PPP. On trouve  $EA=4.14$  min. Les courbes ont en abscisse le temps inter-arrivées (en minutes) et en ordonnée, le nombre d'appels correspondant. L'histogramme observé est comparé à une distribution exponentielle de même moyenne (en tirets).



## Exercice 2 : Coût d'une liaison

On veut comparer le coût d'une liaison avec 2 techniques très différentes : TRANSPAC et TRANSFIX. On ne se préoccupe pas ici des questions de routage des paquets IP, de serveur de nom ou de matériel spécifique (à régler par ailleurs)

### Question 1

*A l'aide des annexes ci-dessous, déterminer le coût d'un accès au débit calculé précédemment selon ces 2 techniques, en distinguant les différents paramètres du coût total.*

Pour les calculs, on supposera que la distance de raccordement est de moins de 10 km entre le CNAM et le fournisseur d'accès.

### Question 2

Par souci de bonne gestion, on souhaite reporter ces coûts sur les usagers.

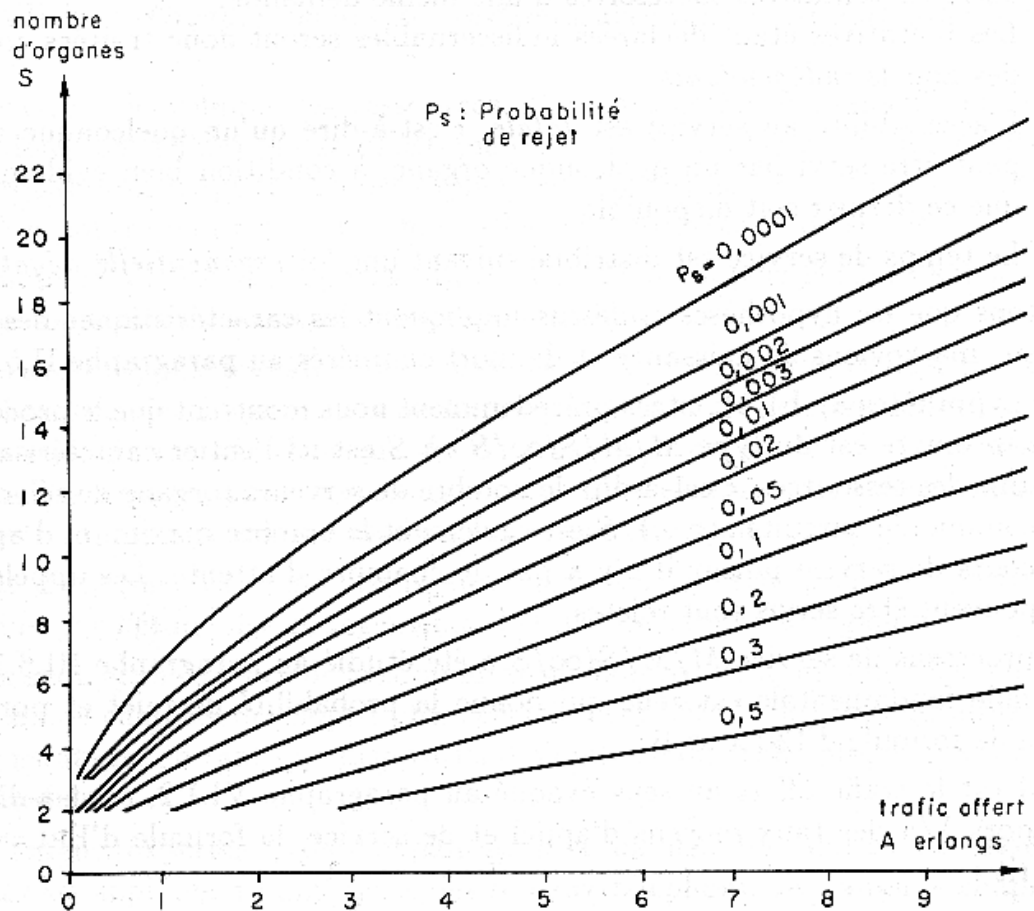
Les frais fixes sont supposés amortis en 3 ans.

*Calculer le prix minimum de l'abonnement d'un usager*

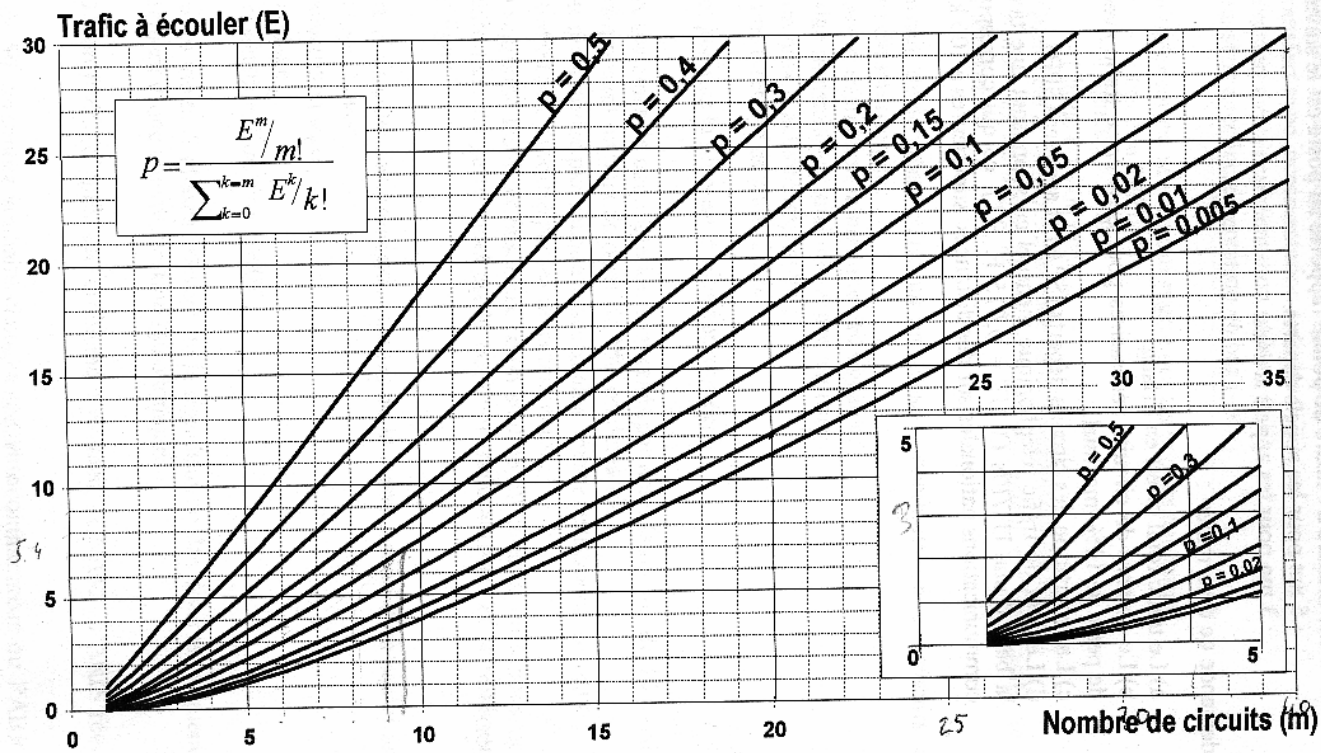
*Comparer ce coût à un abonnement personnel "du marché"*







Extrait de DOYON "Systèmes et réseaux de télécommunication en régime stochastique"



Extrait de MAIMAN & SERVIN "Autoformation en télécoms et réseaux"

RLS	LL POINT A POINT	FRANCE	
	TARIF NON CONTRACTUEL	TELECOM	
TRANSFIX 2.0 1024 Kb/s			
Distance en km : 9... ou pour la calculer C + ENVOI			
COUT	Francs HT	TVA 20.6%	TOTAL TTC
mensuel	7876.00	1622.46	9498.46
bimest.	15752.00	3244.91	18996.91
accès	60000.00	12360.00	72360.00
Autre distance		RETOUR	
Autre type de LL		*RETOUR	
Quitter		SOMMAIRE	

RLS	LL POINT A POINT	FRANC	
	TARIF NON CONTRACTUEL	TELECOM	
TRANSFIX 2.0 768 Kb/s			
Distance en km : 9... ou pour la calculer C + ENVOI			
COUT	Francs HT	TVA 20.6%	TOTAL TT
mensuel	7520.00	1549.12	9069.
bimest.	15040.00	3098.24	18138.
accès	40000.00	8240.00	48240.
Autre distance		RETOUR	
Autre type de LL		*RETOUR	
Quitter		SOMMAIRE	

### Extraits du 3614 RLF (haut) et du Web de Transpac (bas)

**Netscape: Transpac - Services Réseaux**

Back Forward Home Reload Images Open Print Find Stop

Netsite: [http://www.transpac.fr/services/s\\_index.htm](http://www.transpac.fr/services/s_index.htm)

Autres sites  
English version

ACCUEIL

L'ENTREPRISE

GLOBAL INTRANET

SERVICES RÉSEAUX

SERVICES D'ACCÈS

VALEUR AJOUTÉE

SERVICES CLIENTS

SOLUTIONS

ACTUALITÉS

PARTENAIRES

BIBLIOTHÈQUE

RECHERCHE

CONTACT

AIDE

France Telecom  
Transpac

**SERVICES RÉSEAUX**  
▶ SERVICES D'ACCÈS

**1.1.1. Abonnement mensuel France**

Comprend la liaison d'accès au réseau.

Débit d'accès	Prix mensuel
14 400 bit/s	1 630 F
19 200 bit/s	2 200 F
64 Kbit/s	2 400 F
128 Kbit/s (-)	4 700 F
256 Kbit/s (-)	9 200 F

(-) Service non offert localement dans les DOM

Durée initiale d'abonnement : 6 mois.  
Pour les débits supérieurs, de 512 Kbit/s à 2 Mbit/s, consulter les services commerciaux.

Nota : le prix est indépendant de la distance pour les débits inférieurs ou égaux à 64 Kbit/s. Pour les débits supérieurs à 64 Kbit/s, si la distance est supérieure à 15 km, consulter les services commerciaux.

**1.1.2. Frais de mise en service pour accès direct France**

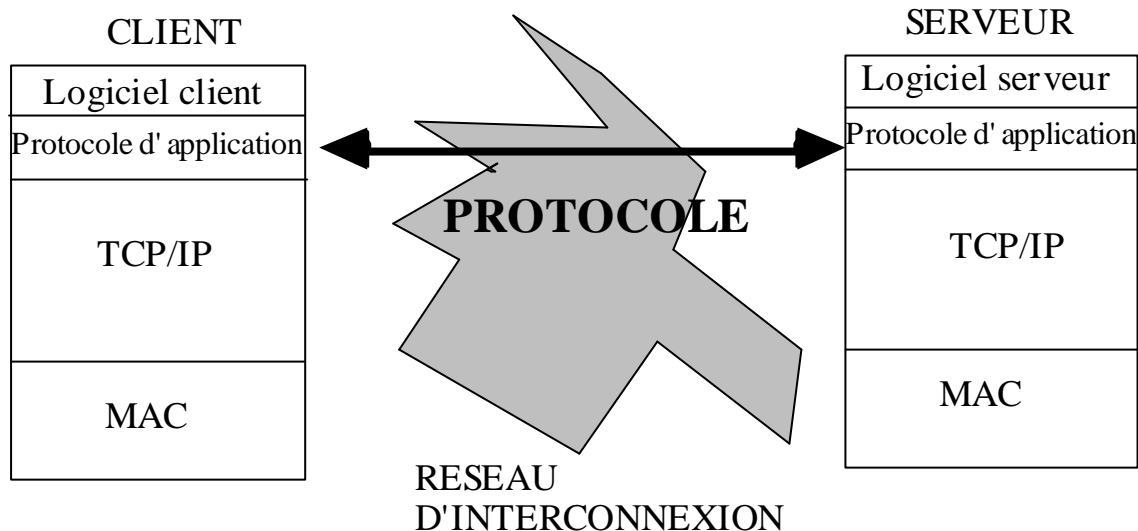
Débits d'accès	Mise en service
14 400 à 19 200 bit/s	6 800 F
64 à 128 Kbit/s	10 000 F
256 Kbit/s	22 000 F

Ces frais sont également applicables lorsqu'il y a modification de débit avec reconstruction de la liaison.

# Utilisation de l'API socket

## Exercice 1 : Le protocole HTTP et le World-Wide-Web

Le but du WWW est de permettre la consultation à distance de documents multi-média hypertextuels. Ces documents sont composés dans un langage de balisage de structure appelé HTML (Hyper Text Markup Language). Il existe de nombreux logiciels clients WWW (Netscape Navigator, Internet Explorer, Mosaic, Lynx,...) ainsi que de nombreux logiciels serveurs (NCSA, Apache, MacHttp, ...)



### Question 1 : Utilisation du client Netscape Navigator

*Lancer Netscape et naviguer dans les documents.*

La commande "View Source" permet de visualiser le source HTML que le serveur a envoyé au client.

*Expliquer sur un exemple de document à quoi correspondent les balises HTML*

La zone de saisie "Location" permet d'indiquer quel document on souhaite consulter.

*Quelle est à votre avis la syntaxe adoptée ? Quel est le rôle des différentes parties ?*

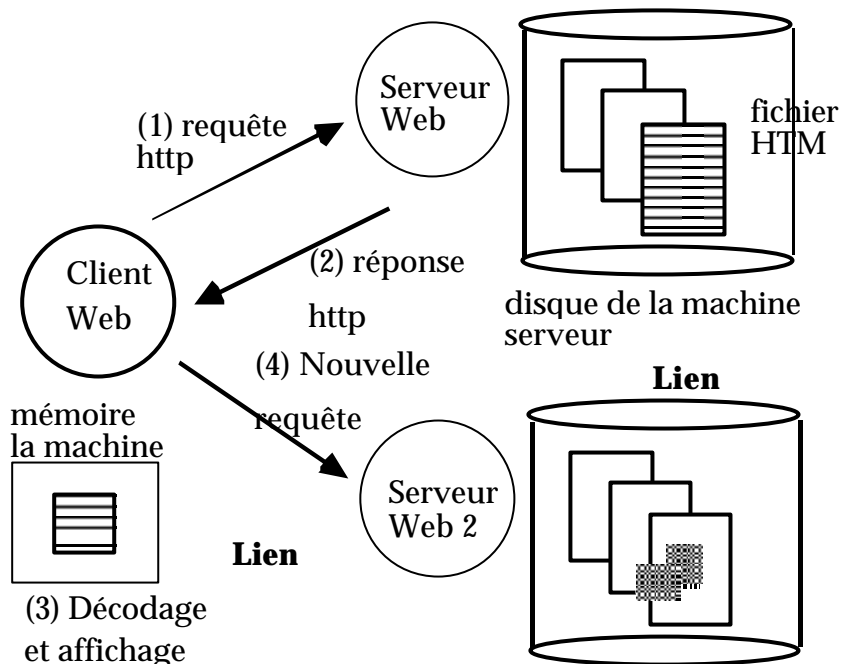
### Question 2 : Le protocole HTTP

Le protocole utilisé par le WWW s'appelle Hyper Text Transfer Protocol (HTTP). Dans sa version actuelle (1.0), il s'agit d'un simple protocole de type "requête-réponse": le client demande au serveur le document HTML et le serveur le renvoie (voir figure).

On peut se connecter directement sur un serveur WWW en se logeant par TELNET sur le port 80 de la machine qui héberge le serveur WWW.

*Lancer le logiciel TELNET en se connectant sur la machine cedric.cnam.fr*

*Pourquoi le système ne demande-t'il pas d'identification ?*



La syntaxe d'une requête GET est `GET <chemin fichier> <protocole>`

*Essayer par exemple `GET /index.html http/1.0` suivi de 2 retour-charriot Que retourne le serveur ?*

*Essayer ensuite `GET /toto.html http/1.0`*

*Que retourne le serveur ? Que se passe-t'il pour les images ?*

## Exercice 2 : Un client HTTP minimal

En utilisant les IPC internet, l'interaction client-serveur se réduit à l'automate suivant :

SERVEUR	CLIENT
<code>socket()</code> Prépare une prise de connexion	<code>socket()</code>
<code>bind()</code> Assigne un numéro de port à une prise	<code>gethostbyname()</code> Donne adresse IP serveur à partir de son nom
<code>listen()</code> Prépare pour des demandes de connexion	
<code>accept()</code> Prend en compte une connexion	<code>connect()</code> Établissement d'une connexion
<code>read()</code> Demande de service + données	<code>write()</code>
<code>write()</code> Réponse+résultats	<code>read()</code>
<code>close()</code> Fermeture/destruction de la prise	<code>close()</code>

Pour utiliser les IPC internet, il faut inclure dans son code C les déclarations suivantes :

```
#include <stdio.h>
#include <signal.h>
#include <ctype.h>
#include <errno.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <netinet/tcp.h>
#include <arpa/inet.h>
```

Voici les primitives nécessaires :

```
/* conversion d'une numéro de port au format interne */
unsigned short int htons(unsigned short int);
/* copie de zone mémoire */
void bcopy (void * src, void * dest, int n) ;
/* Obtenir l'adresse IP d'une machine à partir de son nom */
struct hostent *gethostbyname (char *);
/* Créer une nouvelle socket ; retourne une descripteur de fichier */
int socket (int family, int type, int protocol);
/* Donner une adresse à une socket*/
int bind (int sockfd, struct sockaddr *my_addr, int addrlen);
/* Ouvrir une connexion */
int connect (int sockfd, struct sockaddr *serv_addr, int addrlen);
/* Prépare une socket serveur pour accepter N connections */
int listen (int sockfd, int n);
/* Attend une connexion ; quand une connexion arrive créé une nouvelle socket */
int accept (int sockfd, struct sockaddr *peer, int *paddrlen);
```

Avec les structures de données suivantes:

```
struct hostent {
    char    *h_name;          /* official name of host */
    char    **h_aliases;     /* alias list */
    int     h_addrtype;      /* host address type */
    int     h_length;        /* length of address */
    char    **h_addr_list;   /* list of addresses from name server */
#define h_addr h_addr_list[0] /* address, for backward compatibility */
}

#define __SOCK_SIZE__ 16 /* sizeof(struct sockaddr) */
struct sockaddr_in {
    sa_family_t    sin_family; /* Address family */
    unsigned short int sin_port; /* Port number */
    struct in_addr sin_addr; /* Internet address */
    unsigned char   __pad[__SOCK_SIZE__ - sizeof(short int) -
        sizeof(unsigned short int) - sizeof(struct in_addr)];
};
```

## Question 1

*En utilisant l'automate présenté précédemment, écrire un petit programme en C qui va récupérer le contenu d'un fichier disponible sur un serveur 'httpd', à partir de son URL.*

Ce client 'http' va se connecter au serveur 'httpd' avec une socket en mode TCP, puis va émettre un ordre GET chemin HTTP/1.0, puis affichera le flux d'informations retourné par le serveur.

Exemples d'utilisation de ce programme :

```
%geturl lmil7 /index.html
```

```
%geturl cedric.cnam.fr /ABU/BIB/index.html
```

## Question 2

*Ecrire un script shell **getHREF** qui utilisera le programme précédent pour afficher tous les URL contenu dans le fichier.*

Exemples d'utilisation de ce programme :

```
%getHREF lmi17 /index.html
```

```
%getHREF cedric.cnam.fr /ABU/BIB/index.html
```

## Question 3

Notre client `http geturl` est trop rapide.

*Ecrire une variante de celui-ci qui lit à la vitesse de 1 caractère par seconde toutes les informations envoyées par le serveur http.*

Exemples d'utilisation de ce programme :

```
%lentgeturl lmi17 /index.html >tmp &
```

```
%lentgeturl lmi17.cnam.fr /Meteo/satt0.gif >tmp &
```

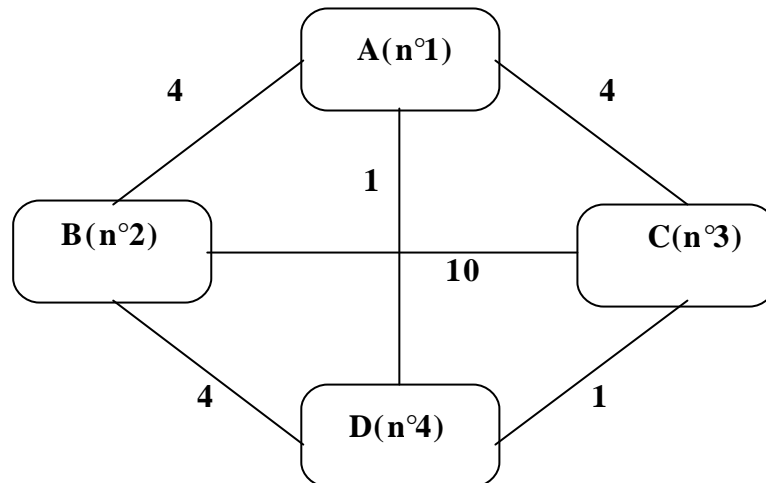
*Visualiser l'état des sockets sur le client et le serveur avec la commande `netstat`.*

*Expliquer l'état des tampons.*

NOTE : Consulter C. YOUNG "Programmation de clients Web avec Perl" O'Reilly 1997 pour écrire des clients HTTP plus sophistiqués.

# Routage RIP

Le graphe ci-dessous représente un réseau informatique : les sommets : A, B, C, D représentent les noeuds de commutation et les arcs les liaisons bidirectionnelles. La valeur portée sur les arcs représente une distance de communication point à point qui est supposée être identique dans les deux sens. Cette distance matérialise un coût de communication qui sert dans la suite de l'ED pour déterminer un meilleur chemin et fabriquer les tables de routage des différents noeuds.



Plus loin dans l'exercice, on utilise des numéros pour désigner les noeuds de commutation : A est le n° 1, B est le n° 2, C est le n° 3, et D est le n° 4.

## Question 1 : Calcul du routage centralisé

Pour calculer le routage optimal on utilise l'algorithme centralisé suivant (qui n'est pas le meilleur algorithme centralisé de calcul de chemin minimal dans un graphe)

*Calculer à l'aide de cet algorithme le routage optimal du réseau*

*Déterminer, en utilisant la matrice P, l'arbre de routage (sink tree) et la table de routage du noeud A*

### CONSTANTES

```
N: entier ; % Nombre de noeuds;
Type Nom_de_noeud: entier dans (1..N); % nom des noeuds de commutation;
C : tableau (N,N) de réels ; % cout de transmission en point à point; C(i,i)=0 pour tout i
    et C(i,j)=+8 si il n'y a pas de liaison entre i et j; quand
    il y en a une, le coût a été porté sur l'arc du graphe ci-
    dessus %;
```

### VARIABLES

```
V: tableau (N,N) de réels ; % A la fin de l'algorithme V(i,j) est égal au coût du chemin
    de valeur minimale de i vers j %;
P: tableau (N,N) de Nom_de_noeuds; % A la fin de l'algorithme P(i,j) est le successeur
    de i dans le chemin optimal de i vers j%;
Iter: entier; % numéro d'itération%;
cout: réel;
i,j,k,r: Nom_de_noeuds;
```





## CORPS DE PROCEDURE (Ford)

```
% Initialisation ;

pour i=1 a N
  pour j=1 a N
    V(i,j) := C(i,j);
    Si C(i,j)?+8 faire
      P(i,j):=j;
    finsi
  finpour
finpour

% Itérer N-1 fois %;
Pour iter=1 a N-1;
  % Pour chaque noeud origine d'un chemin %;
  Pour i=1 a N
    % Pour chaque noeud extrémité d'un chemin %;
    Pour j=1 a N
      cout:=+8;
      % Chercher parmi tous les voisins de i celui par lequel
      passe le meilleur chemin vers j %;
      Pour k=1 a N
        Si C(i,k)?+8 faire
          Si C(i,k)+V(k,j)<cout faire
            cout:=C(i,k)+V(k,j);
            r:=k;
          finsi
        finsi
      fin pour
      %Si la valeur trouvée est meilleure que celle contenue dans
      dans V noter le nouveau chemin %;
      Si V(i,j)> cout faire
        V(i,j):=cout;
        P(i,j):=r;
      finsi
    finpour
  finpour
finpour
```

## Question 2 : Algorithme réparti adaptatif (Mac Quillan)

Dans une version d'Arpanet, le routage adaptatif était réalisé en utilisant un algorithme adaptatif réparti dérivé du précédent. Dans cet algorithme le noeud  $i$  calcule uniquement la  $i$ ème ligne des matrices  $V$  et  $P$  (soit le coût de transmission d'un message de  $i$  vers tous les autres noeuds du réseau et l'adjacent préféré de  $i$  vers tous les noeuds du réseau). Pour cela, il envoie périodiquement à ses voisins  $V(i, \bullet)$  et reçoit de chacun d'entre eux la ligne de  $V$  correspondante. L'algorithme s'adapte aux variations des coûts qui sont mesurés à chaque itération.

```
Algorithme Arpa(i)
cycle
  Attendre T secondes;
  pour tout voisin k de i
    Envoyer V(i,•);
    Recevoir V(k,•);
    Mesurer C(i,k);
  finpour
  -- Les données sont prêtes pour une itération du calcul
```

```

    Appliquer la partie A de l'algorithme précédent pour trouver
        les nouvelles valeurs de V(i,•) et P(i,•);
    Déterminer la nouvelle table de routage de i;
fincycle

```

La mesure avec  $\text{Mesurer } C(i, k)$  peut s'effectuer de plusieurs façons différentes. Par exemple on peut considérer que le coût d'une ligne est infini si sur un hôte, la file de messages en émission vers un destinataire est pleine, et vide en réception depuis celui-ci.

On suppose qu'à l'instant  $t=0$  tous les noeuds ont calculé les valeurs respectives de  $V(i, \bullet)$  et  $P(i, \bullet)$  et la table de routage correspondante. La liaison (3,4) tombe en panne. Chaque noeud commence une étape du cycle de calcul.

Pour réaliser la phase A de l'algorithme le noeud  $i$  calcule, à la  $n$ -ème étape du calcul, une matrice  $S_i^{(n)}$ .

$S_i^{(n)}(k, j)$  est l'évaluation par  $i$  du coût pour aller à  $j$  en passant par  $k$ .

*Quelle relation lie  $S_i^{(n)}(k, j)$ ,  $V_k^{(n-1)}(k, j)$  et  $C^n(i, k)$  (valeur du chemin optimal vers  $j$  calculés par  $k$  au cycle précédent et coût mesuré par  $i$  au cycle courant) ?*

*En déduire la relation liant  $S_i^{(n)}$  et  $V^{(n)}(i, \cdot)$*

*Appliquer l'algorithme pour la première itération (numérotée  $n$ ).*

Il est recommandé de retracer le graphe à grande échelle et d'associer au noeud  $i$  la matrice  $S_i$  (voir pages suivantes).

### Question 3

Pendant la première itération, un paquet part d'un ordinateur hôte connecté au noeud de commutation 1 pour être transmis à un hôte connecté au noeud 3.

*Que se passe-t-il ? Compléter les éléments ci-dessous*

$$C_{n-1} = \begin{pmatrix} 0 & 4 & 4 & 1 \\ 4 & 0 & 10 & 4 \\ 4 & 10 & 0 & \infty \\ 1 & 4 & \infty & 0 \end{pmatrix} \quad V_{n-1} = \begin{pmatrix} 0 & 4 & 2 & 1 \\ 4 & 0 & 5 & 4 \\ 2 & 5 & 0 & 1 \\ 1 & 4 & 1 & 0 \end{pmatrix} \text{ obtenus à la question 1}$$

$$S_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \end{pmatrix} \quad \begin{matrix} V(1, \bullet) = ( \\ P(1, \bullet) = ( \end{matrix} \quad S_2 = \begin{pmatrix} \cdot & & & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \\ \cdot & & & \end{pmatrix} \quad \begin{matrix} V(2, \bullet) = ( \\ P(2, \bullet) = ( \end{matrix}$$

$$S_3 = \begin{pmatrix} \cdot & & & \\ \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \end{pmatrix} \quad \begin{matrix} V(3, \bullet) = ( \\ P(3, \bullet) = ( \end{matrix} \quad S_4 = \begin{pmatrix} \cdot & & & \\ \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad \begin{matrix} V(4, \bullet) = ( \\ P(4, \bullet) = ( \end{matrix}$$

Les valeurs de V et P sont stabilisées après plusieurs itérations si on suppose que les coûts ne sont plus modifiés durant cette phase de calcul. Les itérations n+1, n+2, n+3 sont données ci-dessous.

$$V_n = \begin{pmatrix} \phantom{0} \\ \phantom{0} \\ \phantom{0} \\ \phantom{0} \end{pmatrix}$$

$$S_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \end{pmatrix} \quad \begin{matrix} V(1, \bullet) = ( \phantom{0} \phantom{0} \phantom{0} \phantom{0} ) \\ P(1, \bullet) = ( \phantom{0} \phantom{0} \phantom{0} \phantom{0} ) \end{matrix} \quad S_2 = \begin{pmatrix} 4 & \cdot & 6 & 5 \\ \cdot & \cdot & \cdot & \cdot \\ 14 & \cdot & 10 & 15 \\ 5 & \cdot & 7 & 4 \end{pmatrix} \quad \begin{matrix} V(2, \bullet) = (4 \ 0 \ 6 \ 4) \\ P(2, \bullet) = (1 \ 2 \ 1 \ 4) \end{matrix}$$

$$S_3 = \begin{pmatrix} 4 & 8 & \cdot & 5 \\ 14 & 10 & \cdot & 14 \\ \cdot & \cdot & \cdot & \cdot \\ \infty & \infty & \cdot & \infty \end{pmatrix} \quad \begin{matrix} V(3, \bullet) = (4 \ 8 \ 0 \ 5) \\ P(3, \bullet) = (1 \ 1 \ 3 \ 1) \end{matrix} \quad S_4 = \begin{pmatrix} 1 & 5 & 3 & \cdot \\ 8 & 4 & 9 & \cdot \\ \infty & \infty & \infty & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad \begin{matrix} V(4, \bullet) = (1 \ 4 \ 3 \ 0) \\ P(4, \bullet) = (1 \ 2 \ 1 \ 4) \end{matrix}$$

$$V_{n+1} = \begin{pmatrix} 0 & 4 & 4 & 1 \\ 4 & 0 & 6 & 4 \\ 4 & 8 & 0 & 5 \\ 1 & 4 & 3 & 0 \end{pmatrix}$$

$$S_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & 4 & 10 & 8 \\ \cdot & 12 & 4 & 9 \\ \cdot & 5 & 4 & 1 \end{pmatrix} \quad \begin{matrix} V(1, \bullet) = (0 \ 4 \ 4 \ 1) \\ P(1, \bullet) = (1 \ 2 \ 3 \ 4) \end{matrix} \quad S_2 = \begin{pmatrix} 4 & \cdot & 8 & 5 \\ \cdot & \cdot & \cdot & \cdot \\ 14 & \cdot & 10 & 15 \\ 5 & \cdot & 7 & 4 \end{pmatrix} \quad \begin{matrix} V(2, \bullet) = (4 \ 0 \ 7 \ 4) \\ P(2, \bullet) = (1 \ 2 \ 4 \ 4) \end{matrix}$$

$$S_3 = \begin{pmatrix} 4 & 8 & \cdot & 5 \\ 14 & 10 & \cdot & 14 \\ \cdot & \cdot & \cdot & \cdot \\ \infty & \infty & \cdot & \infty \end{pmatrix} \quad \begin{matrix} V(3, \bullet) = (4 \ 8 \ 0 \ 5) \\ P(3, \bullet) = (1 \ 1 \ 3 \ 1) \end{matrix} \quad S_4 = \begin{pmatrix} 1 & 5 & 5 & \cdot \\ 8 & 4 & 10 & \cdot \\ \infty & \infty & \infty & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad \begin{matrix} V(4, \bullet) = (1 \ 4 \ 5 \ 0) \\ P(4, \bullet) = (1 \ 2 \ 1 \ 4) \end{matrix}$$

$$V_{n+2} = \begin{pmatrix} 0 & 4 & 4 & 1 \\ 4 & 0 & 7 & 4 \\ 4 & 8 & 0 & 5 \\ 1 & 4 & 5 & 0 \end{pmatrix}$$

$$S_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & 4 & 11 & 8 \\ \cdot & 12 & 4 & 9 \\ \cdot & 5 & 6 & 1 \end{pmatrix} \quad \begin{matrix} V(1, \bullet) = (0 \ 4 \ 4 \ 1) \\ P(1, \bullet) = (1 \ 2 \ 3 \ 4) \end{matrix} \quad S_2 = \begin{pmatrix} 4 & \cdot & 8 & 5 \\ \cdot & \cdot & \cdot & \cdot \\ 14 & \cdot & 10 & 15 \\ 5 & \cdot & 9 & 4 \end{pmatrix} \quad \begin{matrix} V(2, \bullet) = (4 \ 0 \ 8 \ 4) \\ P(2, \bullet) = (1 \ 2 \ 1 \ 4) \end{matrix}$$

$$S_3 = \begin{pmatrix} 4 & 8 & \cdot & 5 \\ 14 & 10 & \cdot & 14 \\ \cdot & \cdot & \cdot & \cdot \\ \infty & \infty & \cdot & \infty \end{pmatrix} \quad \begin{matrix} V(3, \bullet) = (4 \ 8 \ 0 \ 5) \\ P(3, \bullet) = (1 \ 1 \ 3 \ 1) \end{matrix} \quad S_4 = \begin{pmatrix} 1 & 5 & 5 & \cdot \\ 8 & 4 & 11 & \cdot \\ \infty & \infty & \infty & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad \begin{matrix} V(4, \bullet) = (1 \ 4 \ 5 \ 0) \\ P(4, \bullet) = (1 \ 2 \ 1 \ 4) \end{matrix}$$

$$V_{n+3} = \begin{pmatrix} 0 & 4 & 4 & 1 \\ 4 & 0 & 8 & 4 \\ 4 & 8 & 0 & 5 \\ 1 & 4 & 5 & 0 \end{pmatrix}$$

Cette solution est optimale, l'itération suivante donnerait le même résultat !!!

Remarque : Il est possible que certaines erreurs se soient glissées dans les calculs, mais elles ne gênent en rien la réponse à la dernière question.

# Fonctionnalités TCP/UDP-IP

Pour chacun des protocoles IPV4 et TCP indiquez s'ils possèdent les fonctionnalités suivantes. Si oui indiquez au moyen de quels champs et de quel mécanisme, la fonctionnalité considérée est réalisée sur un datagramme ou sur un segment.

1) Contrôle de séquence (livraison en séquence) en IP ? En TCP ? Retransmission sur erreur en IP V4 (Contrôle d'erreur)? En TCP ? Contrôle de flux en IP ? En TCP ?

La trame Ethernet suivante a été prélevée par un programme d'écoute d'une voie Ethernet. Cette trame est éditée par lignes de 16 octets en hexadécimal. C'est une trame au format standard Ethernet DIX et non au format IEEE 802.3. Le préambule de la trame Ethernet avec le délimiteur de début de trame n'est pas inclus dans la trace. Le code polynomial de contrôle (CRC Ethernet) est représentée par xxxx xxxx.

```
00: 0800 2001 b432 0800 2000 61f3 0800 4500
16: 0028 0c39 0000 1e06 8077 c009 c80b c009
32: c801 0450 0015 0006 e802 0080 3e08 5010
48: 1000 64be 0000 0000 0000 0000 xxxx xxxx
```

2) Entête Ethernet : Quelles sont les adresses Ethernet source et destination de la trame ? Ou se trouve le type de protocole réseau encapsulé dans la trame Ethernet ? Quelle est sa valeur (à quel protocole de réseau doit être délivré la charge utile de la trame) ?

3) Entête IP : Le datagramme IP contient-il des options ? Pourquoi ?

4) Entête IP : S'agit-il du premier fragment d'un datagramme fragmenté ? S'agit-il du dernier fragment d'un datagramme fragmenté ? Pourquoi ?

5) Entête IP : Quelle est la valeur du champ TTL ('Time to live', temps restant à séjourner) ? Comment détermine t'on que le protocole de transport qui utilise ce datagramme IP est TCP ?

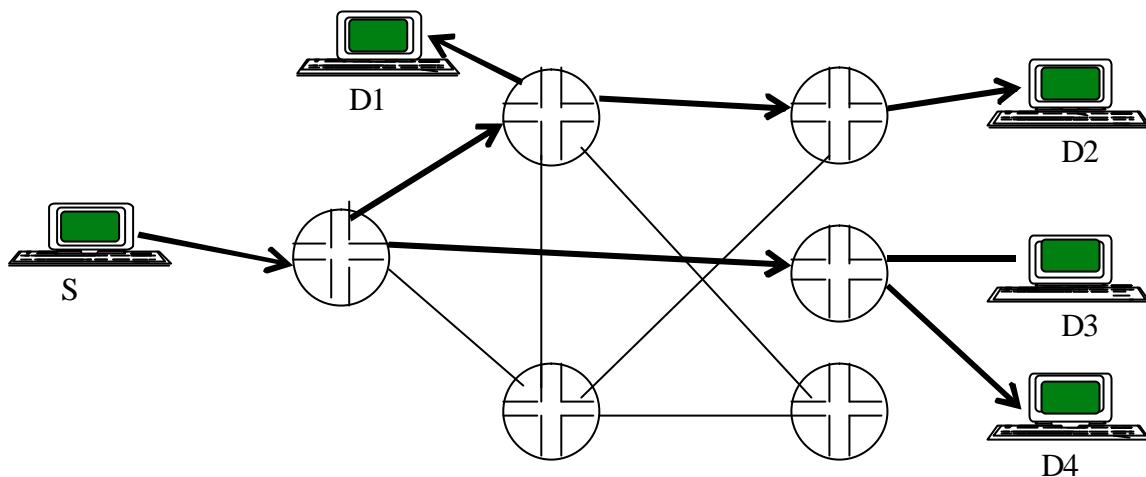
6) Entête TCP : Quels sont les numéros de port source et destination de ce segment?

7) Entête TCP : Quels sont les indicateurs positionnés par le message ('flags'). Quel est la valeur et à quoi servent des numéros de séquence, d'acquiescement et le pointeur urgent contenus dans le segment?

8) Entête TCP : Quel est le nombre d'octets pouvant être émis en anticipation (quel est le crédit) mentionné dans ce segment ?

# Routage en diffusion sur Internet

Dans ce problème on étudie la diffusion sur groupe (multicast) dans l'Internet. La figure suivante représente un site émetteur (une source de messages S) et des sites destinataires (D1, D2, D3, D4). On a représenté le réseau avec des hôtes, des routeurs, des liens qui sont utilisés dans une diffusion sur groupes (traits gras) et d'autres liens et routeurs inutilisés.



1) Le principe fondamental d'un routage en diffusion sur groupe consiste à construire un arbre couvrant à coût minimum enraciné au site source et dont les feuilles sont les sites destinataires. Sur l'arbre, pour diffuser aux destinataires, on ne transmet qu'une copie du message par liaison utilisée. On cherche à comparer la solution en point à point à la solution en diffusion sur une arbre, en utilisant la métrique Internet du nombre de sauts.

1.1) Pour le réseau de la figure précédente, si l'on réalise quatre communications en point à point pour aller de S aux quatre destinataires combien de sauts doit-on effectuer ?

1.2) Si l'on utilise l'arbre couvrant en diffusion, combien de saut doit-on effectuer ?

1.3) Supposons qu'un routage en diffusion utilise un arbre binaire pour atteindre  $2^*N$  destinataires, combien de sauts doit-on effectuer en mode point à point ?

1.4) Sur un arbre binaire permettant d'atteindre  $2^*N$  destinataires, combien de sauts doit-on effectuer en mode diffusion sur l'arbre ?

1.5) Que conclure quant aux performances relatives des deux solutions ?

## 2) Adresses IP de diffusion.

2.1) L'adressage IPV4 utilise dans sa version de base différentes classes d'adresses. Quelle est le nom de la classe qui est prévue pour la diffusion à des groupes de destinataires (le multicast)? Quelles sont les adresses utilisables pour définir des groupes de diffusion?

2.2) De combien d'adresses différentes peut-on ainsi disposer pour adresser des groupes en Ipv4?

2.3) Les adresses multicast IP peuvent servir à délivrer des messages en diffusion au moyen de réseaux locaux type Ethernet. Ethernet dispose également d'un adressage multicast.

Pour établir automatiquement une correspondance entre adresse IP multicast et adresses Ethernet multicast une technique normalisée consiste à copier 23 bits de poids faible de l'adresse IP multicast pour fabriquer 23 bits de l'adresse multicast Ethernet qui lui correspond. Sur le schéma suivant on représente une adresse Ethernet multicast avec le préfixe constant caractéristique de la conversion IP multicast vers Ethernet multicast et un bit à 0 qui ramène à 23 le nombre de bits significatifs dans les 24 bits de la partie droite.

```
0           23           47
|           |           |
1000 0000 0000 0000 0111 1010 xxxx xxx0 xxxx xxxx xxxx xxxx
```

Cette présentation correspond au codage des adresses Ethernet lorsqu'elles circulent sur les fils (le bit 0 est envoyé en premier en codage grand boutiste). Pourquoi le premier bit est-il obligatoirement à 1 ?

2.4) La représentation officielle des adresses Ethernet est telle que les 6 octets sont numérotés de la gauche vers la droite (grand boutiste) mais les bits à l'intérieur des octets sont numérotés de la droite vers la gauche (petit boutiste). Lorsque l'on édite une adresse Ethernet, dans la représentation officielle (dite en mémoire), les adresses multicast Ethernet sont donc notées en inversant l'ordre des bits dans les octets. L'adresse Ethernet multicast avec le préfixe constant caractéristique de la conversion IP multicast vers Ethernet multicast devient donc :

```
0           23           47
|           |           |
0000 0001 0000 0000 0101 1110 0xxx xxxx xxxx xxxx xxxx xxxx
```

Le domaine d'adressage est donc défini dans les normes par l'intervalle 01:00:5e:00:00:00 à 01:00:5e:7f:ff:ff

Soient les adresses multicast IP 224.144.8.5 et 225.144.8.5 (en hexadécimal e0.90.08.05 et e1.90.08.05). Donner les adresses multicast Ethernet correspondantes sachant que l'on recopie purement et simplement les 23 bits de la partie droite de l'adresse IP multicast dans l'adresse Ethernet multicast (pour répondre, en cas de doute on peut éventuellement représenter sous forme binaire les adresses) ? Comment résoudre le problème posé par l'utilisation simultanée de ces deux adresses dans le même réseau.

### 3) Gestion des abonnements

3.1) Quel est le protocole de la suite Internet qui prend en charge la gestion des groupes en IP V4?

3.2) Quelles sont ses principales fonctions?

#### 4) Routage en diffusion.

4.1) Le problème du routage en diffusion consiste à atteindre à partir d'une source un groupe de destinataires. L'un des protocoles de routage en diffusion sur l'internet s'appelle DVMRP ("Distance Vector Multicast Routing Protocol"). Le protocole DVMRP est donc un routage à vecteur de distance qui utilise un principe voisin du protocole RIP ("Routing Information Protocol"). Rappelez les principes des protocoles à vecteur de distance pour entretenir une table des chemins à coût minimum dans un réseau?

4.2) En DVMRP, pour construire l'arbre de diffusion, périodiquement un routeur source (un routeur de rattachement d'un hôte source) émet vers ses routeurs voisins un message indiquant qu'il a un flot de messages en diffusion à transmettre. Les différents routeurs atteints réémettent à leur tour ce message vers leurs voisins. Comment appelle-t-on une telle stratégie de circulation des messages d'indication de flot ?

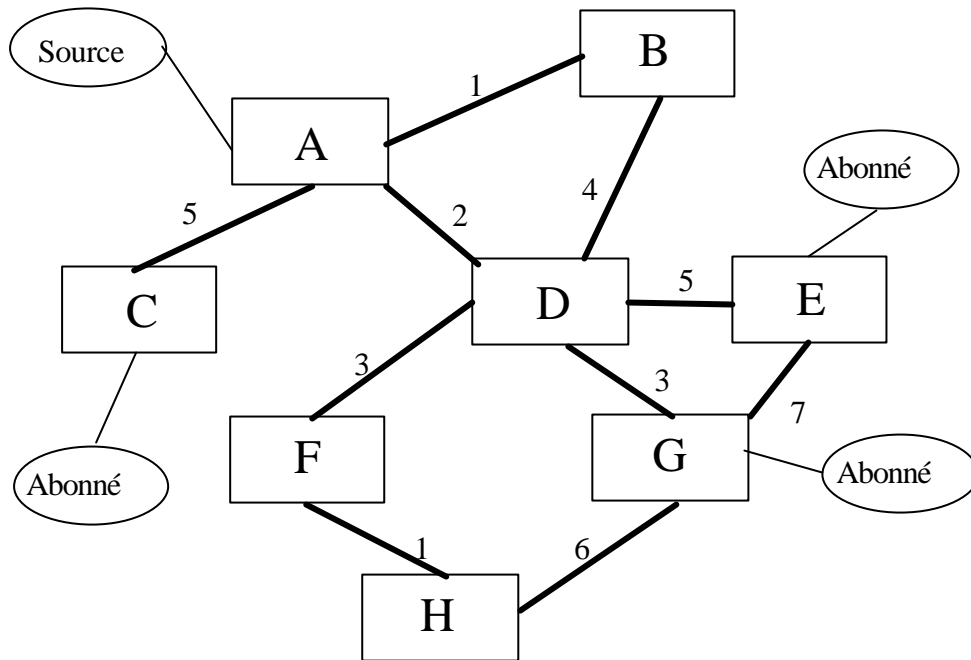
4.3) En fait chaque routeur du réseau n'accepte un message d'indication de flot de diffusion et ne le réémet vers ses voisins que s'il provient du routeur voisin qui se trouve sur le chemin à coût minimum vers la source. Les messages provenant des autres voisins sont ignorés. Pourquoi est-ce que cette stratégie évite l'explosion combinatoire du nombre des messages?

Pour construire l'arbre couvrant à coût minimum, DVMRP fonctionne en deux phases. Dans la première phase, DVMRP construit un arbre couvrant à coût minimum du routeur source vers tous les routeurs ("minimum spanning tree").

Dans la seconde phase DVMRP procède à l'élagage de l'arbre couvrant. Lorsqu'un routeur est une feuille de l'arbre couvrant (il ne relaie pas de messages vers un autre routeur) et qu'il n'est pas destinataire (il n'y a pas d'abonné connecté à ce routeur à qui les messages d'un flot de diffusion doivent être délivrés) alors ce routeur n'a pas à recevoir le flot de diffusion. Il peut être retiré de l'arbre de diffusion. Ce routeur émet un message à son père dans l'arbre qui est appelé message d'élagage. De proche en proche l'élagage se poursuit jusqu'à obtenir un arbre utilisable.

4.4) Sur le réseau suivant qui comporte 8 routeurs notés A,B,C,D,E,F,G,H, on a mentionné les coûts des arêtes. Quelle est la circulation des messages dans la première phase? On présente la réponse sous la forme d'un ensemble de lignes (X , Y) ou X est l'émetteur et Y le destinataire d'un message. On ajoute pour chaque message l'indication Y retransmet le message ou Y ne retransmet pas. Par exemple la première ligne de la réponse est: (A , B) B retransmet le message.





- 4.5) Quel est l'arbre couvrant obtenu après circulation des messages d'indication de flot ?
- 4.6) Quelle est la circulation des messages d'élagage?
- 4.7) Quel est l'arbre de diffusion finalement construit après circulation des messages d'élagage?

# Protocole de transport RTP

Dans les vingt premières années de son existence le réseau Internet a été utilisé pour des applications de transmission de données informatiques en mode asynchrone comme les transferts de fichiers, les transferts de courriers électroniques, l'accès à des documents. Ensuite, l'utilisation d'Internet a évolué progressivement vers des applications multimédia à flux continu. Des applications comme le téléphone, la diffusion radio ou télévision sont considérées comme des applications Internet utilisant les quatre couches basses de cette architecture réseau. Dans cet ensemble, on distingue deux types de transmissions. Le cas le plus simple est celui des données à flux continu pouvant être stockées avant d'être délivrées (plusieurs secondes à plusieurs dizaines de seconde comme dans le cas de la radio, de la télévision, on parle de 'streaming'). Un cas plus difficile est celui des données multimédia à délivrance en 'temps réel' comme le téléphone ou la visio-conférence.

Ce problème s'intéresse à la transmission des données au niveau transport pour des applications multimédia sur Internet et en particulier au protocole de transport RTP (Real-time Transport Protocol RFC 3550 Juillet 2003).

## Question 1

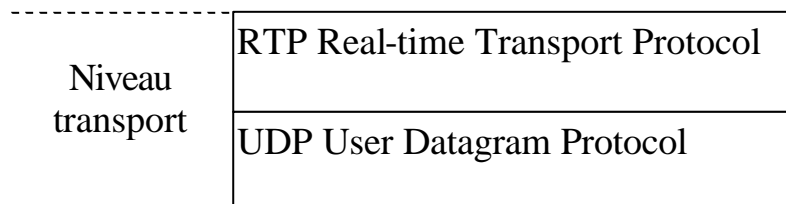
*Dans le domaine des données multimédia en flux continu on s'intéresse surtout à la transmission de données en mode synchrone. Rappelez la définition d'une transmission synchrone. Donnez quelques exemples de communication en mode synchrone au niveau physique.*

Des applications Internet souhaitant échanger des flux continus peuvent envisager d'utiliser comme protocole de transport TCP (pour la transmission de données synchrones).

## Question 2

*Indiquez plusieurs problèmes liés aux caractéristiques de TCP. On examinera les caractéristiques habituelles des protocoles concernant, la livraison en séquence, les mécanismes de contrôle d'erreur, de contrôle de flux, de contrôle de congestion, et dans le cas précis la délivrance synchrone.*

Le protocole de transport temps réel RTP a choisi de s'appuyer sur le service du protocole UDP pour la transmission de données synchrones. Donc dans une transmission avec RTP le niveau transport comprend les deux protocoles RTP et UDP selon l'architecture suivante.



## Question 3

*Pourquoi avoir choisi le protocole UDP comme protocole sous jacent à RTP ?*

L'entête d'un message de données RTP comprend cinq champs:

- Le champ type ('Payload Type') décrit le type de la charge utile transportée (sur 7 bits).
- Le champ numéro de séquence ('Sequence Number') est le numéro de séquence du message RTP. Il est incrémenté à chaque nouvel envoi d'un message RTP (sur 16 bits).
- Le champ estampille ('Timestamp') sur 32 bits. Ce champ reflète l'instant d'échantillonnage du premier octet de la charge utile. Supposons par exemple que pour un certain type de codage du son, un message RTP transporte 40 échantillons de son prélevés 44000 fois par seconde alors la valeur du champ estampille progresse de 40 à chaque nouveau message.
- Le champ identifiant de la source ('Synchronization Source Identifier') sur 32 bits. C'est un identifiant choisi aléatoirement qui identifie une source de données RTP. On peut en effet avoir sur le même hôte plusieurs flots de données transmises en même temps vers le même destinataire.
- Différents indicateurs (numéro de version, existence d'octets de bourrage, existence d'extension d'entête ...) sont également présents dans l'entête. Ils ne sont pas détaillés dans ce sujet.

#### Question 4

*Selon la norme RTP, la zone type de charge utile de l'entête ayant pour valeur 0 est attribué au codage MIC avec la loi  $m$  à 64 kb/s (PCM,  $m$  law 64) du téléphone numérique. Rappelez les principes de base du MIC (échantillonnage, quantification, codage)?*

#### Question 5

*L'utilisation du codage MIC suppose que codage et le décodage soient effectués par des horloges synchronisées (comme c'est le cas dans les réseaux RNIS). Dans le cas d'une transmission avec RTP/UDP/IP, l'application qui reçoit le flux MIC va utiliser un buffer pour amortir la gigue. Quelle sera alors l'influence de la dérive des horloges sur le buffer ?*

#### Question 6

*Est-on obligé de maintenir une latence constante durant toute la durée de la communication, pour chaque échantillon ? Le codage de la voix nécessite-t-il donc une transmission complètement synchrone ? Comment dans ce cas gérer le simplement le problème de dérive d'horloge ?*

Des techniques de détection de silences sont parfois introduites directement dans le format de codage du média, mais ce n'est pas le cas du MIC (codé en G.711). Ainsi, RTP propose d'introduire un type de payload appelé *Comfort Noise* (RFC 3389) pour introduire un « Silence Insertion Descriptor ».

Les protocoles comme SIP (pour la signalisation dans la téléphonie sur IP, RFC 3261, Juin 2002) ou SAP (RFC 2974, Octobre 2000) pour annoncer des sessions Multimédia (conférence, diffusion, etc) sont des protocoles servant à «initialiser» une communication avec des flux multimédia. Ces protocoles utilisent SDP (Session Description Protocol, RFC 2327) pour présenter les informations nécessaires à l'établissement de session RTP.

Dans un paquet SDP, la description d'une session se fait au format texte et la description est la forme <type>=<value>.

Voici un extrait de description de session :

m=audio 49170 RTP/AVP 0 13

m=video 51372 RTP/AVP 31

m=application 32416 udp whiteboard

Pour les valeurs « audio » et « vidéo » : m=<audio ou vidéo> <port utilisé> <protocole de transport> <type de payload 1> <type de payload 2> ... <type de payload n>

Pour « application », remplacer <type de payload> par le nom de l'application.

### **Question 7**

*Le payload numéro « 0 » correspond au codage G.711 (MIC) et le 13 au « Comfort Noise » et le 31 au codage vidéo h.261. Quel sera alors le nombre de session RTP ouverte ?*

### **Question 8**

*Donner des exemples d'applications dans lesquelles le « Comfort Noise » n'est pas applicable.*

### **Question 9**

*Comment un utilisateur du protocole RTP peut-il utiliser les informations dont il dispose pour délivrer correctement (de manière synchrone) les unités d'informations transportées ?*

### **Question 10**

*On s'intéresse maintenant au traitement des erreurs de transmission dans le protocole RTP. On considère tout d'abord la pile des protocoles utilisés. Quels sont les mécanismes de traitement des erreurs mis en œuvre dans les différents protocoles Internet (aux niveaux physique, liaison, réseau et transport avec UDP) ?*

### **Question 11**

*Avec l'ensemble des informations qui ont été données dans ce texte sur RTP (format de l'entête RTP, utilisation par RTP de UDP et des protocoles Internet) comment le destinataire d'un message peut-il détecter une erreur de transmission sur un message ?*

### **Question 12**

*Compte tenu des objectifs de transmission synchrone, quel mécanisme de traitement des erreurs de transmission (codes détecteurs d'erreur avec retransmission, codes correcteurs d'erreurs) doit être privilégié par un utilisateur d'un protocole de transport pour des données multimédia en flux continu comme RTP ?*

L'une des solutions proposée pour traiter les erreurs dans des flux continus consiste à rajouter en émission le mécanisme suivant. Après avoir émis  $n$  messages (chaque message contient  $k$  échantillons de son ou d'image), un utilisateur RTP émet un message  $n+1$  dont la valeur est le ou exclusif des  $n$  messages précédents (la parité longitudinale de  $k$  échantillons).

### **Question 13**

*Comment utiliser cette parité dans le cadre du traitement des erreurs (examinez les possibilités offertes en détection comme en correction en prenant en compte les solutions des questions 5 et 6) ?*