le cnam

Année universitaire 2019-2020

SUJET RSX101 : Réseaux et Protocoles pour l'Internet

Examen 2e session du 05/09/2020

Responsable : *E. GRESSIER-SOUDAN*

Durée : 3 heures + 0h45 spécifiquement pour gérer l'environnement d'examen à distance

Consignes

Tous documents autorisés

Les étudiants ne doivent pas communiquer entre eux.

Contrevenir à toute obligation correspond à un risque de 5 ans d'exclusion du CNAM.

Pour chaque question il est demandé une justification précise de votre réponse.
Le barème de cet examen correspond à une notation sur 23 points dont 3 points optionnels

Sujet de **22 pages**, celle-ci comprise.

Important : Les étudiants répondent sur le sujet d'examen. Ils impriment une version pdf de leur composition et la remette sur moodle, éventuellement l'envoient par mail à : eric.gressier_soudan@cnam.fr à des fins de secours, mais c'est la copie sur moodle qui fait référence.

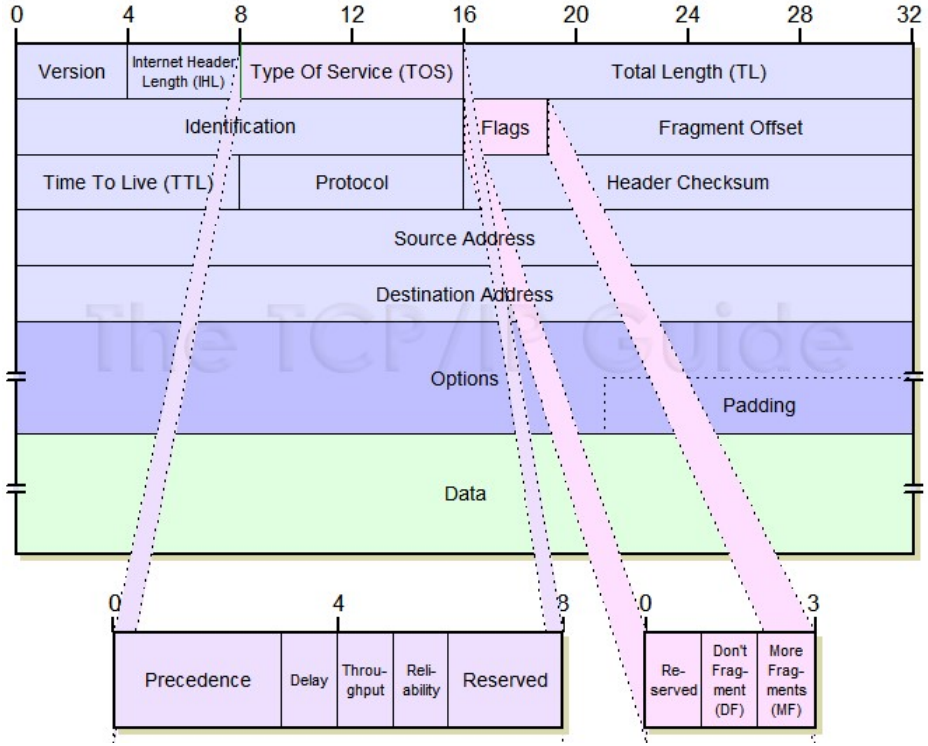
Une fois les 3h écoulées et le temps additionnel pour gérer sujet et copie avec réponse terminés, il n'est plus possible de remettre sa réponse sur moodle. **Au total vous disposez de 3h45 pour l'ensemble de l'épreuve** au lieu de 3h dans des conditions présentielles normales**.**

Exercice 1 : Mise en œuvre de la QoS dans un routeur (7 points)

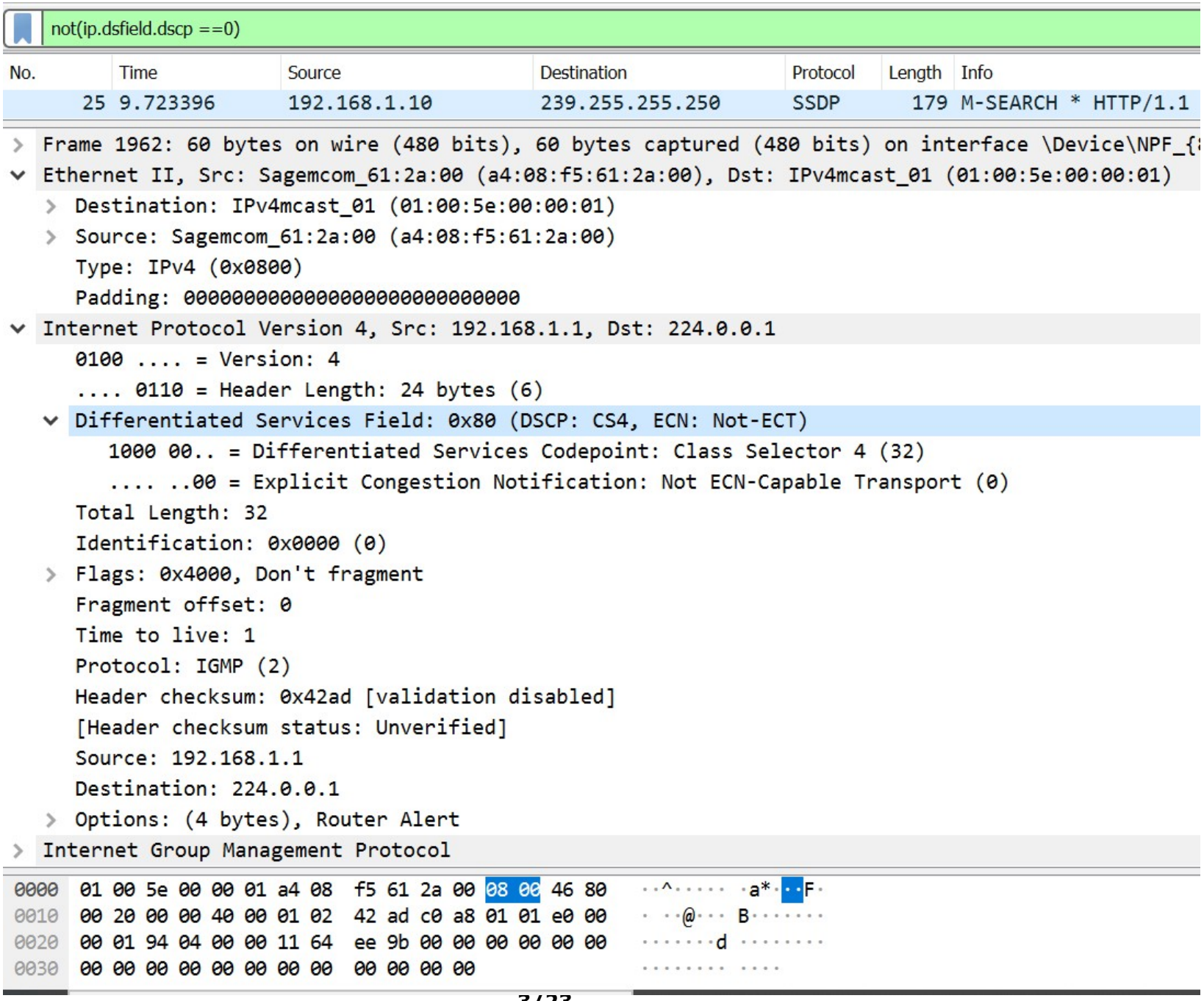
On donne la structure d'une trame Ethernet :

Adresse destination	Adresse source	Type	Informations	FCS
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

On donne la structure d'un datagramme IP dont son entête en détail, consulté le 23 décembre 2013, Source http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm :



Question 1 : On s'intéresse à une trace Wireshark qui est extraite d'un trafic Teams capturé en mars 2020. On s'attache en particulier à la trame 25 donnée ci-après. **(2 points)**


not(ip.dsfield.dscp ==0)
No. Time Source Destination Protocol Length Info
25 9.723396 192.168.1.10 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
Frame 1962: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{
Ethernet II, Src: Sagemcom_61:2a:00 (a4:08:f5:61:2a:00), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
Destination: IPv4mcast_01 (01:00:5e:00:00:01)
Source: Sagemcom_61:2a:00 (a4:08:f5:61:2a:00)
Type: IPv4 (0x0800)
Padding: 00000000000000000000000000
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 224.0.0.1
0100 .... = Version: 4
.... 0110 = Header Length: 24 bytes (6)
Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
1000 00.. = Differentiated Services Codepoint: Class Selector 4 (32)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 32
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 1
Protocol: IGMP (2)
Header checksum: 0x42ad [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.1
Destination: 224.0.0.1
Options: (4 bytes), Router Alert
Internet Group Management Protocol
0000 01 00 5e 00 00 01 a4 08 f5 61 2a 00 08 00 46 80
0010 00 20 00 00 40 00 01 02 42 ad c0 a8 01 01 e0 00
0020 00 01 94 04 00 00 11 64 ee 9b 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

Voilà son extraction en hexadécimal :

```
0000            01 00 5E 00 00 01 A4 08    F5 61 5d 1f 08 00 46 80

0010            00 20 00 00 40 00 01 02    42 AD C0 A8 01 01 E0 00

0020            00 01 94 04 00 00 11 64    EE 9B 00 00 00 00 00 00

0030            00 00 00 00 00 00 00 00    00 00 00 00
```

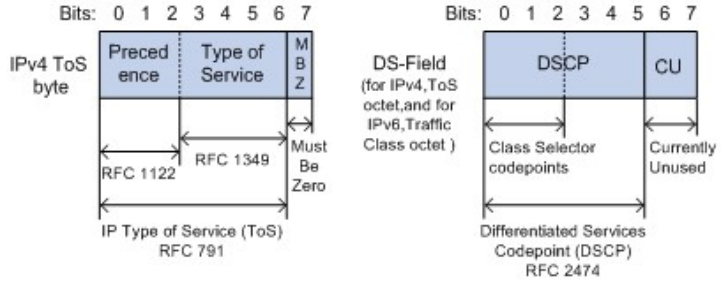
Attention la colonne la plus à gauche numérote les lignes et cette numérotation est hexadécimale.

- Délimiter l'entête du datagramme IP dans la capture en hexadécimal ci-dessous. Ne pas hésiter à utiliser des couleurs différentes pour que votre réponse soit facile à lire. **(0,25 point)**

Retrouver les champs suivants dans la trace hexadécimale ci-dessus :

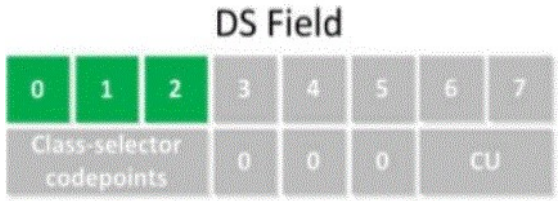
- Quelle est l'adresse Ethernet destination en **hexadécimal** ? **(0,25 point)**
- Quelle est l'adresse Ethernet source en **hexadécimal** ? **(0,25 point)**
- Quelle est la version du protocole IP en **décimal** ? **(0,25 point)**
- Quelle est la longueur de l'entête IP en **décimal** ? **(0,25 point)**
- Quelle est l'adresse IP source en **hexadécimal** ? **(0,25 point)**
- Quelle est l'adresse IP destination en **hexadécimal** ? **(0,25 point)**
- Quelle est la longueur totale du datagramme **en décimal** ? **(0,25 point)**

Question 2 : On se concentre sur la partie QoS (Quamlity of Service, Qualité de Service en français). La QoS est associée au 2ème octet de l'entête IP. Dans la trame 25, il vaut 80 en hexadécimal ou 1000 0000 en binaire. Ce champ peut s'interpréter de deux façons différentes d'après la figure ci-après suivant les RFC qui servent à l'interpréter :



source https://techhub.hpe.com/eginfolib/networking/docs/switches/10500/cg/5200-1877_acl-qos_cg/content/470792642.htm (consultée le 18/08/2020)

https://www.slideshare.net/NetworkersHome1/ip-precedence-dscp-values-quality-of-service-qos (consultée le 18/08/2020) en donne une lecture plus fine dans l'interprétation DSCP :



Pour chaque valeur de "CScodepoint" correspond un comportement particulier du routeur appelé PHB (Per Hop Behavior). On appelle ce PHB, une classe de service. La même source donne un tableau des correspondances entre champ CS (Class-Selector) et Précédence du champ ToS :

Class selector name	DSCP value	IP precedence Value	IP precedence name
Default/CS0	000000	000	Routine
CS1	001000	001	Priority
CS2	010000	101	Immediate
CS3	011000	011	Flash
CS4	100000	100	Flash Override
CS5	101000	101	Critic/Critical
CS6	110000	110	Internetwork Control
CS6	111000	111	Network Control

As you can see, CS1 is the same as "priority" and CS4 is the same as "**flash override**". We can use this for compatibility between the "old" TOS byte and the "new" DS field.
The default PHB and these class-selector PHBs are both described in RFC 2474 from 1998.

Tableau 1. Définition des Class Selector.

Le champ DSCP évolue encore avec la RFC2597 qui définit 4 classes de PHB particuliers AF (Assured Forwarding PHB Group) selon la même source :

Avec les bits 3, 4 et 5, une probabilité d'élimination en cas de saturation de file de messages du routeur est spécifiée. Ce champ est défini dans le tableau ci-après (toujours d'après la même source) :

Possible values that we can use:

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
	AF11	AF21	AF31	AF41
Medium	001100	010100	011100	100100
	AF12	AF22	AF32	AF42
High	001110	010110	011110	100110
	AF13	AF23	AF33	AF43

Class 4 has the highest priority. For example, any packet from class 4 will always get better treatment than a packet from class 3.

Some vendors prefer to use decimal values instead of AF11, AF32, etc. A quick way to convert the AF value to a decimal value is by using the 8x + 2y formula where X = class and Y = drop probability. For example, AF31 in decimal is 8 x 3 + 2 x 1 = 26.

Tableau 2. Définition des PHB AF.

Est-ce que la classe CS4 indiquée par Wireshark, et qui appartient au tableau 1, se retrouve dans le tableau 2 ? Si oui sous quel AF ? Si non à votre avis pourquoi et dans quelle colonne AF devrait/pourrait-elle être placée ? Est-ce que c'est la même chose pour les autres classes CS du tableau 1 ? **(1 point)**

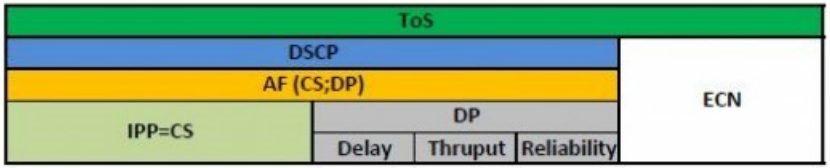
Question 3 : On s'intéresse a la relation entre classes et types d'applications pour configurer les files de messages d'un routeur. **(3 points)**
A l'ensemble des classes données dans les deux tableaux ci-dessus, il faut en ajouter deux autres. Best Effort (BE) ou Default (DF) donne la marque 000 000 en binaire. L'autre classe, c'est Expedited Forwarding (EF) qui vaut 101110 en binaire ou 46[1] en décimal.

[1] Passer de 101110 à 46 en décimal n'est pas immédiat. Pour trouver 46, il faut ajouter '00" devant 101110. En effet, 00101110 donne 2^E en hexadécimal, qui fait bien 46 en décimal.

Peer-to-peer media-sharing applications (KaZaa, Morpheus, Groekster, Napster, iMesh, and so on), gaming applications (Doom, Quake, Unreal Tournament, and so on), and any entertainment video applications.

QoS Values Calculator v3

CoS = Class of Service
DSCP = Differentiated Services Code Point
ToS = Type of Service
AF = Assured Forwarding
IPP = IP Precedence
CS = Class Selector
DP = Drop Probability
ECN = Explicit Congestion Notification



	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
ToS	128	64	32	16	8	4	2	1
DSCP	32	16	8	4	2	1		
CoS=IPP	4	2	1					

Application	CoS=IPP	AF	DSCP	ToS	ToS HEX	DP	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
Best Effort	0	0	0	0	0		0	0	0	0	0	0	0	0
Scavanger	1	CS1	8	32	20		0	0	1	0	0	0	0	0
Bulk Data	1	AF11	10	40	28	Low	0	0	1	0	1	0	0	0
	1	AF12	12	48	30	Medium	0	0	1	1	0	0	0	0
	1	AF13	14	56	38	High	0	0	1	1	1	0	0	0
Network Mgmt.	2	CS2	16	64	40		0	1	0	0	0	0	0	0
Transaction Data	2	AF21	18	72	48	Low	0	1	0	0	1	0	0	0
	2	AF22	20	80	50	Medium	0	1	0	1	0	0	0	0
	2	AF23	22	88	58	High	0	1	0	1	1	0	0	0
Call Signaling	3	CS3	24	96	60		0	1	1	0	0	0	0	0
Mission-Critical	3	AF31	26	104	68	Low	0	1	1	0	1	0	0	0
Streaming Video	3	AF32	28	112	70	Medium	0	1	1	1	0	0	0	0
	3	AF33	30	120	78	High	0	1	1	1	1	0	0	0
	4	CS4	32	128	80		1	0	0	0	0	0	0	0
Interactive Video	4	AF41	34	136	88	Low	1	0	0	0	1	0	0	0
	4	AF42	36	144	90	Medium	1	0	0	1	0	0	0	0
	4	AF43	38	152	98	High	1	0	0	1	1	0	0	0
	5	CS5	40	160	A0		1	0	1	0	0	0	0	0
Voice	5	EF	46	184	B8		1	0	1	1	1	0	0	0
Routing	6	CS6	48	192	C0		1	1	0	0	0	0	0	0
	7	CS7	56	224	E0		1	1	1	0	0	0	0	0

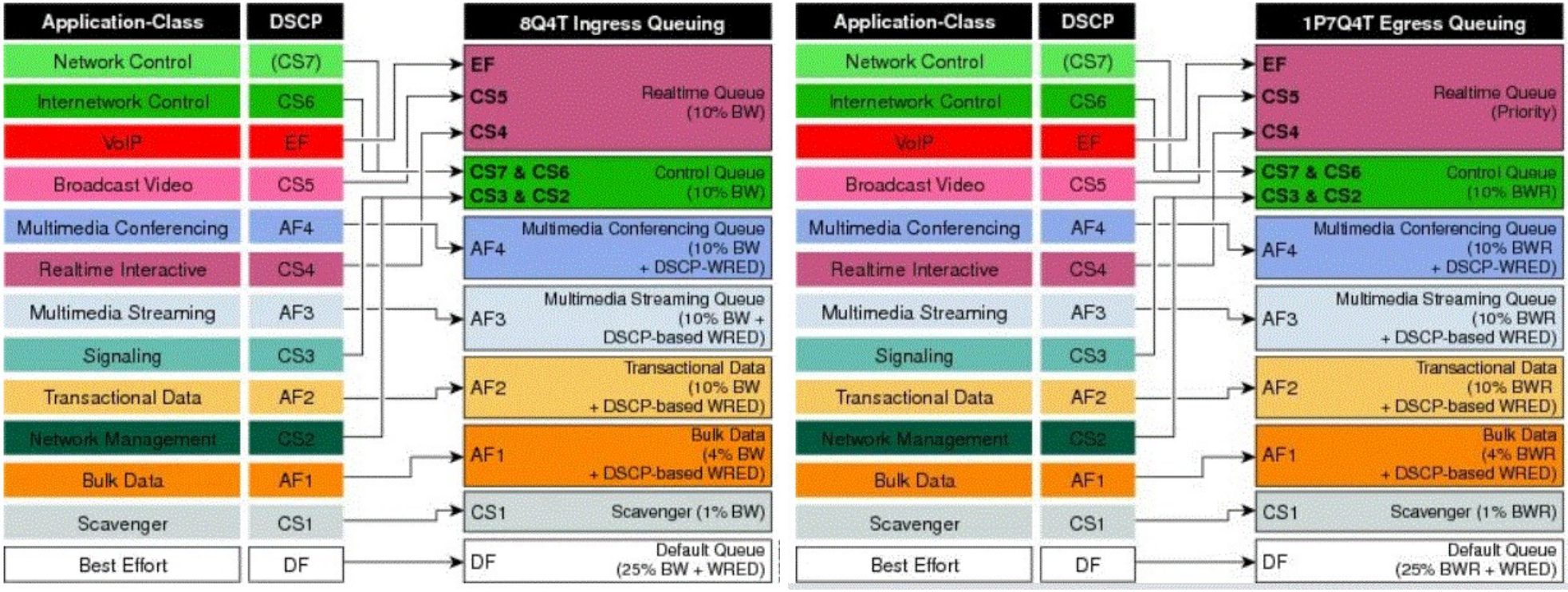
Version:
v2 - ToS in HEX added
v3 - Applications description and DSCP 0 added

NetContractor

Relation entre les différents marquages dans le champ ToS/DSCP, et aussi dans celui de la couche liaison IEEE802.1Q/p (CoS)

source : http://www.netcontractor.pl/blog/?tag=dscp (consultée le 18/08/2020)

Les files de messages associées aux interfaces réseau d'un routeur, dans le cadre d'une gestion de QoS, ont deux fonctions : la mise en œuvre de l'ordonnancement des messages pour le respect du SLA client de bout en bout, et, la politique d'évitement de congestion des files. On associe un modèle de gestion de file, par classification, pour les datagrammes entrants[2](ingress) et un pour les datagrammes sortants (egress) :



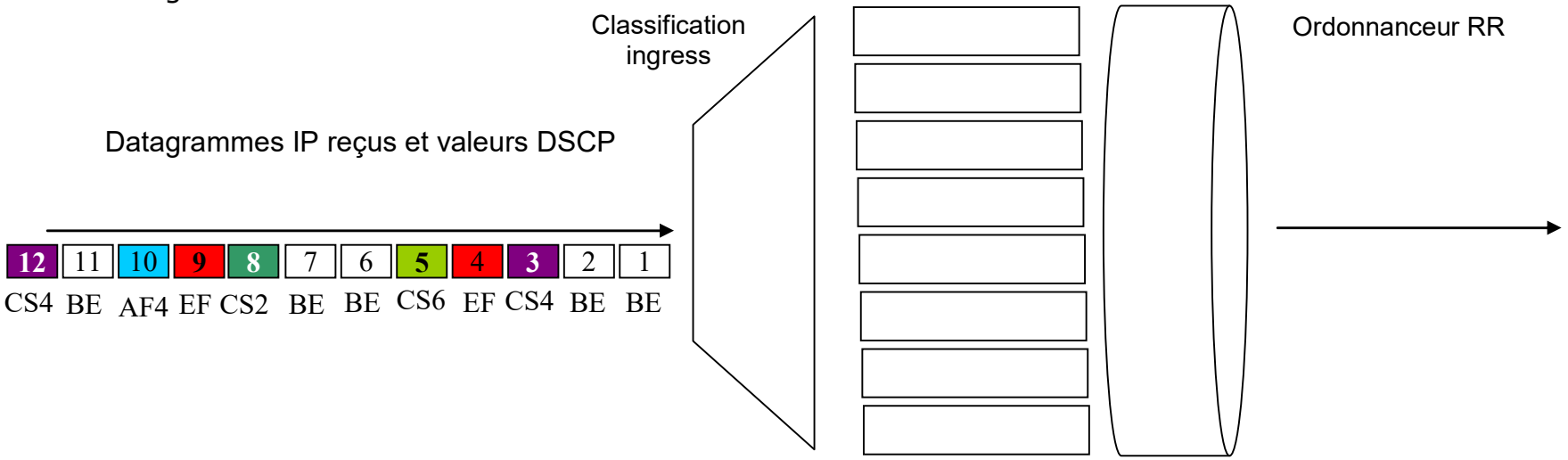
Légendes :

- BW : Bandwidth, débit cible
- WRED : Weighted Random Early Detection
- 8Q4T : 8Q-8 files sans gestion de priorités; 4T-4 seuils peuvent être définis par file
- 1P7Q4T : 1P-une file avec priorité ; 7Q-7 files sans gestion de priorités, 4T-4 seuils peuvent être définis par file

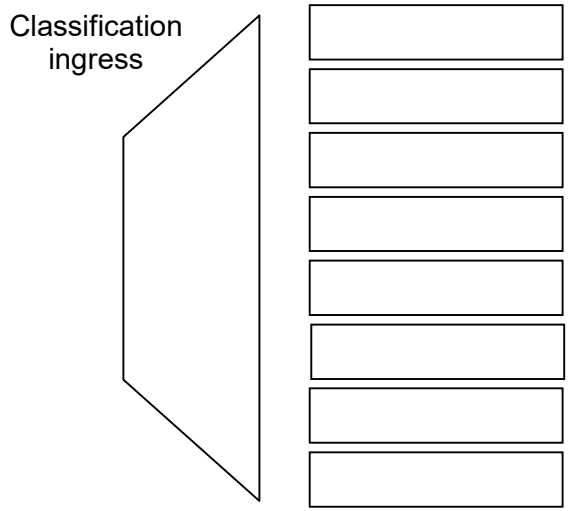
On s'intéresse à l'ordonnancement résultant sur les files d'entrées et de sortir sur un flux de datagramme traversant le routeur. Sur la file d'entrée on ordonnance avec une politique WRR (Weighted Round Robin).

[2] La source des 2 figures est https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/qoscampuscat6500sup2taag.html (consultée le 18/08/2020)

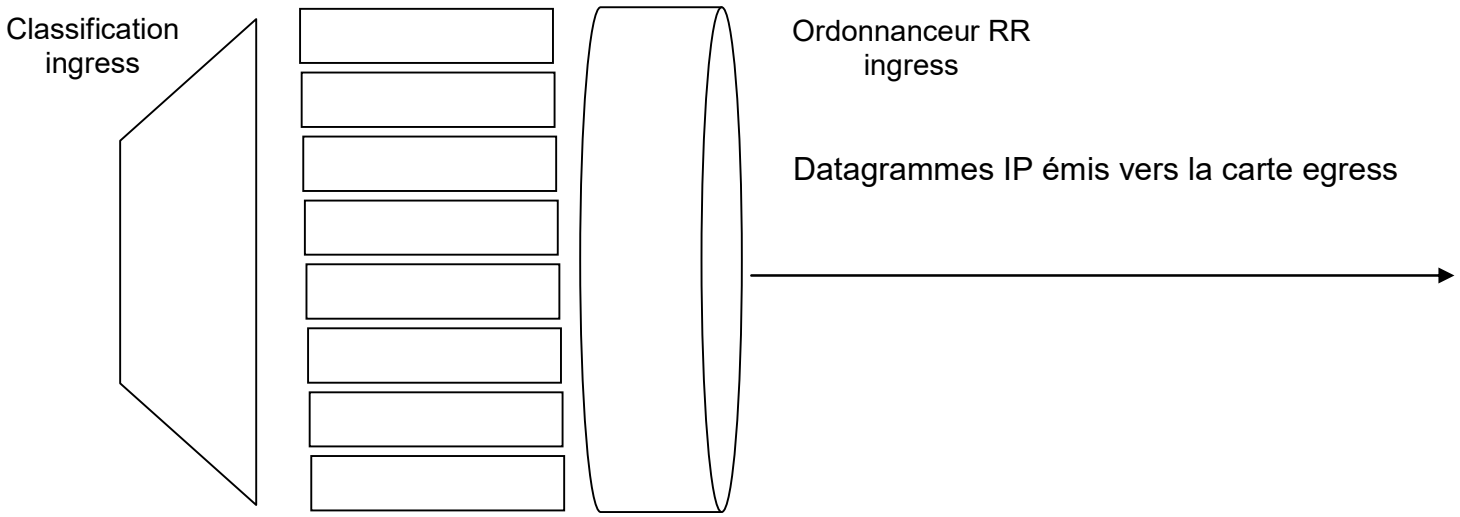
Soit le Flux de datagrammes IP suivant sur la carte en entrée :



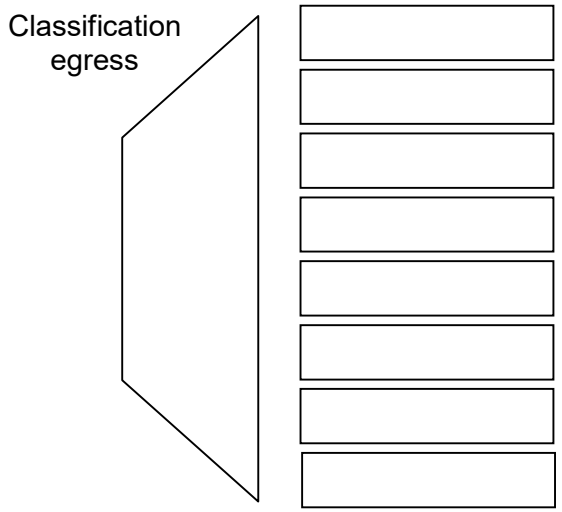
Donner la classification obtenue dans les 8 files conformément au modèle **ingress** présenté ci-dessus en complétant le schéma ci-après. **(0,5point)**



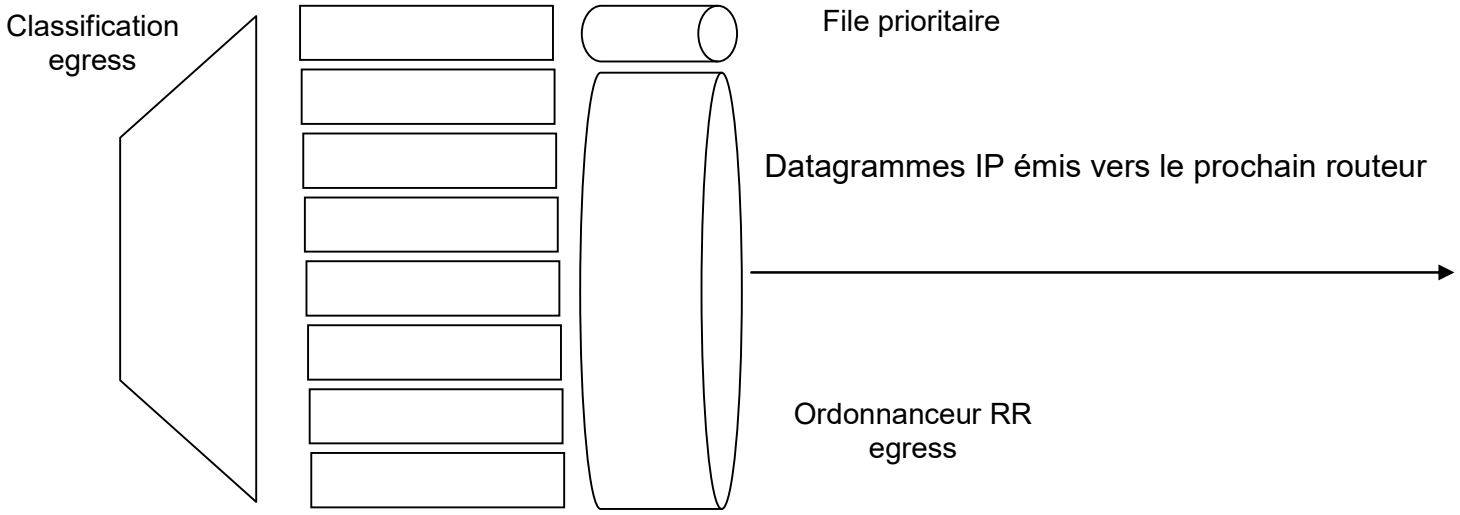
Donner le flux des datagrammes IP sortant de l'ordonnanceur RR (Round Robin) du modèle **ingress** en complétant le schéma ci-après. On supposera que l'ordonnanceur s'exécute une fois les différentes files remplies par le flux arrivant. **(1 point)**



On suppose que le flux de datagrammes IP se dirige vers la carte de sortie qui met en œuvre le modèle egress. Remplir le schéma ci-après correspondant à la classification des datagrammes. **(0,5 point)**



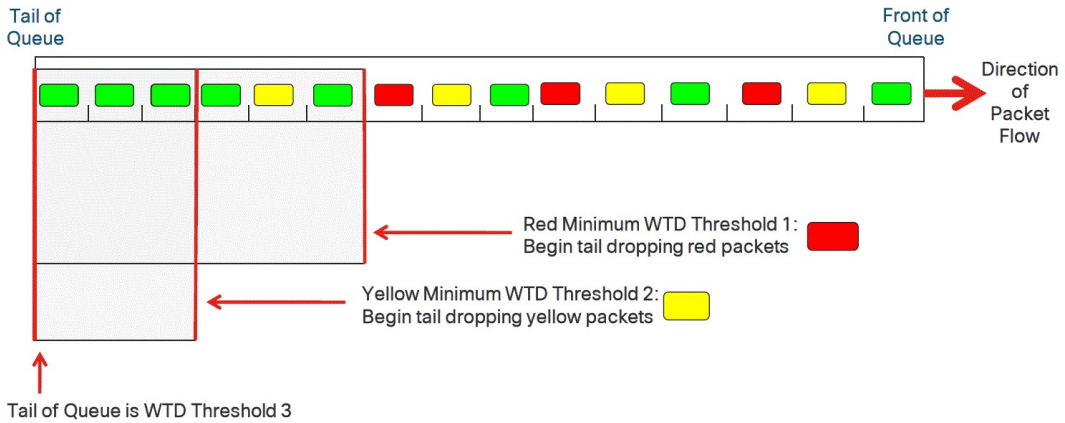
Donner le flux des datagrammes IP sortant de l'ordonnancement du modèle **egress** en complétant le schéma ci-après. On supposera que l'ordonnanceur s'exécute une fois les différentes files remplies par le flux arrivant. **(1 point)**



Question 4 : Comparaison de politiques de contrôle de congestion des files de messages des équipements. **(1 point)**
Cisco propose par défaut deux politiques de gestion de la congestion : Weighted Tail Drop (WTD), et WRED. Les deux stratégies sont rappelées ci-dessous. Comparer les en donnant les avantages et les inconvénients que vous y voyez.

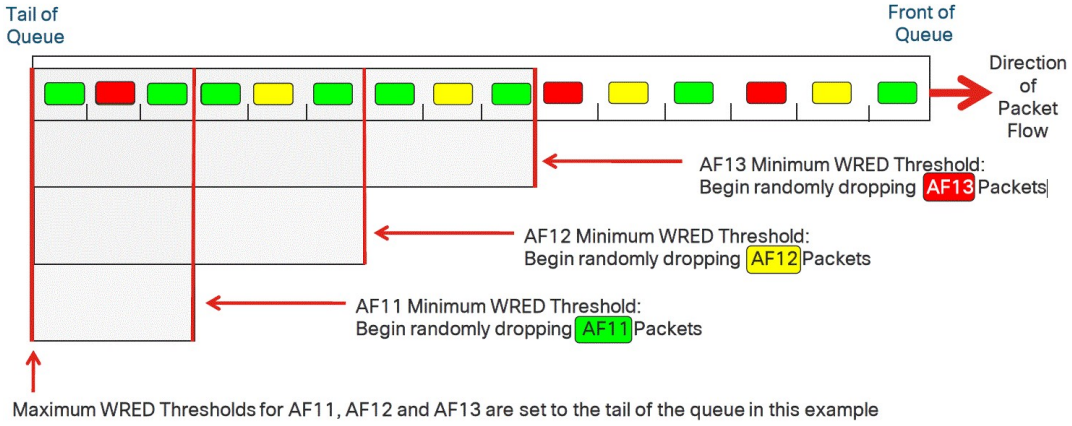
Weighted Tail Drop (WTD) Operation

3T WTD Example



Weighted Random Early Detect (WRED) Operation

3T WRED Example



Exercice 2 : Fermeture de connexion d'un Protocole de Transport (13 points)

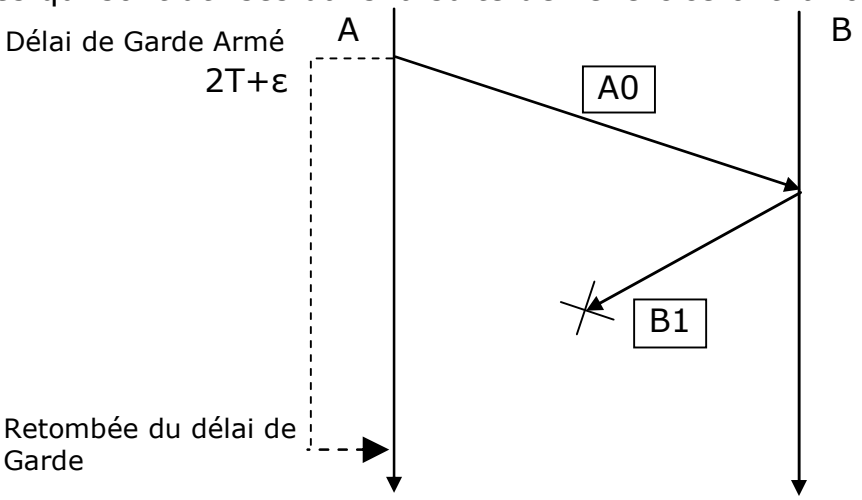
Sujet d'examen rédigé d'après un sujet original inventé[3] par le professeur S. Natkin dans les années 90 pour l'ue NFP104, ancêtre de RSX101, puisque NFP104 existait bien avant sa création. Le créateur de la toute première ue de réseaux au Cnam a été Louis Pouzin, il a été aidé par un des membres du projet Cyclade semble-t-il.

On désire définir un protocole de fermeture négociée d'une connexion de Transport. On a 2 entités de Transport : A et B. Une des 2 entités est à l'initiative de la fermeture de connexion, on supposera que c'est A.

A la fin du protocole, quand les 2 entités A et B ont fermé la connexion, les quatre propriétés suivantes doivent être vérifiées :

- **P1 : B a la certitude que A va fermer la connexion**
- **P2 : A a la certitude que B a la certitude que A va fermer la connexion**
- **P3 : Ni A ni B ne restent bloqués en attente de message**
- **P4 : Le protocole de fermeture de connexion s'exécute en un nombre fini de messages.**

Les diagrammes qui sont utilisés dans la suite de l'exercice ont la forme suivante :



Le diagramme ci-dessus représente un échange de messages entre A et B. A envoie le message A0 qui parvient à B. La réponse B1 envoyée de B vers A est perdue. Au moment où A a envoyé A0, il a armé un délai de garde, de valeur 2T+ε millisecondes (ms), qui retombe suite à l'absence de la réponse B0 attendue.

Question 1 : (1 point)

A et B ont ouvert une connexion de transport. On suppose que le réseau est parfaitement fiable et que le délai pour transmettre un message est T ms. A et B savent que le réseau est parfaitement fiable et que les messages sont acheminés dans un délai borné.

Soit le comportement de A :

```
Début
Envoyer A0;
Fermer la connexion;
Fin
```

[3] Le texte original a été très retravaillé afin que l'énoncé soit plus progressif et pour coller au cours de Transport de RSX101.

Soit le comportement de B :

```
Début
Evénement E;
Attendre E;
Si (E == message A0)
     Alors Fermer la connexion
     Sinon Recevoir Message
Finsi;
Fin
```

Les 4 propriétés énoncées ci-dessus sont-elles vérifiées par les comportements de A et B ? Expliquer pourquoi.

Question 2 : (3 points)

On suppose toujours que le délai d'acheminement d'un message est borné dans le temps. Lorsqu'un message arrive à destination, il a mis au maximum T ms.
Par contre, les messages ont une probabilité non nulle d'être perdus.

On fonde la solution sur la suite d'échanges suivante :
A envoie "je désire fermer la connexion" (message A0)
B répond "j'ai compris que toi A voulait fermer la connexion" (message B1)
A répond "j'ai compris que toi B avait compris que moi A je voulais fermer la connexion" (message A1)
B répond "j'ai compris que toi A avait compris que moi B avait compris que toi A voulait fermer la connexion" (message B2)
Et ainsi de suite…

2.1. Compte tenu de la perte possible de messages, montrer que les propriétés "P1 ET P2" ne peuvent être vérifiées avec certitude. On examine les solutions comportant un ou deux envois de messages au plus. (1 point)

2.2. Supposons qu'il existe une solution en N+1 messages telle que P1 ET P2 soient vérifiées de façon certaine. Comme le N+1ème message peut être perdu, en conclure qu'il existe une solution avec N messages. (1 point)

2.3. En déduire à partir des réponses aux questions 2.1 et 2.2 qu'il n'existe pas de solution qui vérifie les propriétés P1 et P2 de façon certaine. On dit alors que le problème n'a pas de solution déterministe. (1 point)

Dans la suite de l'exercice on va considérer que des pertes de message peuvent se produire avec une certaine probabilité. On bascule donc dans un univers probabiliste.
A partir de maintenant, on note p la probabilité qu'un message se perde en cours de transmission.

Question 3: (2 points)
3.1. Pour N messages envoyés quelle est la probabilité R qu'aucun message n'arrive à destination ? On suppose que la perte d'un message est un événement indépendant d'une autre perte de message. (0,5 point)

3.2. En déduire la probabilité Q pour qu'au moins un message arrive à destination. (0,5 point)

3.3. Calculer Q pour N = 2 et p = 0,5 puis p = 0,1. (0,5 point)

3.4. Pour N messages envoyés quelle est la probabilité S pour que tous les messages arrivent à destination. (0,5 point)

Question 4: (3 points)
Toutes les variables et constantes dans les algorithmes sont des entiers.

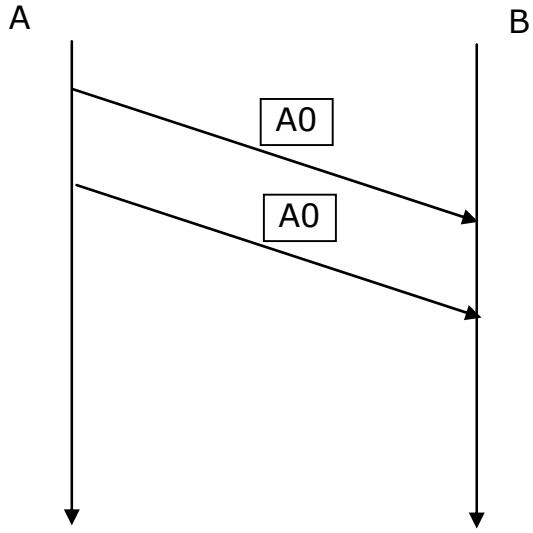
On construit une solution sur la base suivante :

Soit le comportement de A :
```
Début
Constante N;
K := 1 ;
Tant que K ≤ N Faire
     Envoyer A0;
     K := K + 1;
Fin Tant que
Fermer la connexion;
Fin
```

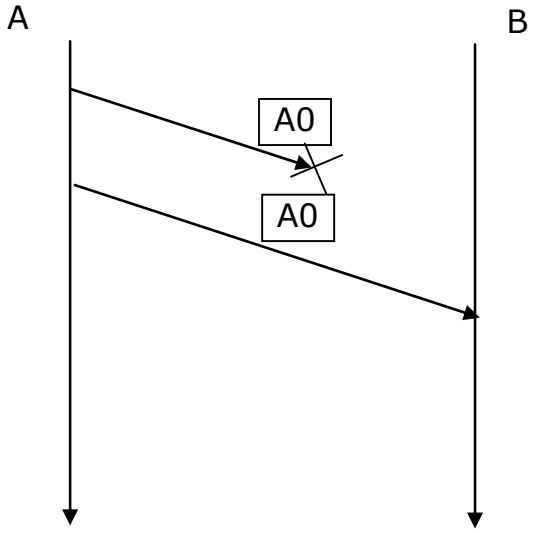
Soit le comportement de B :
```
Début
Evénement E;
Attendre E;
Si (E == message A0)
     Alors Fermer la connexion
     Sinon Recevoir Message
Finsi;
Fin
```

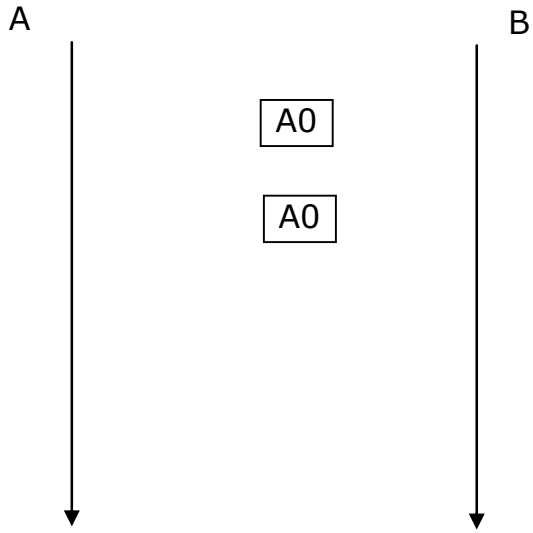
4.1. Pour N = 2 compléter les 4 scénarii suivants si nécessaire, avec les comportements protocolaires spécifiés ci-dessus en tenant compte de tous les cas de pertes possibles. (0,5 point)

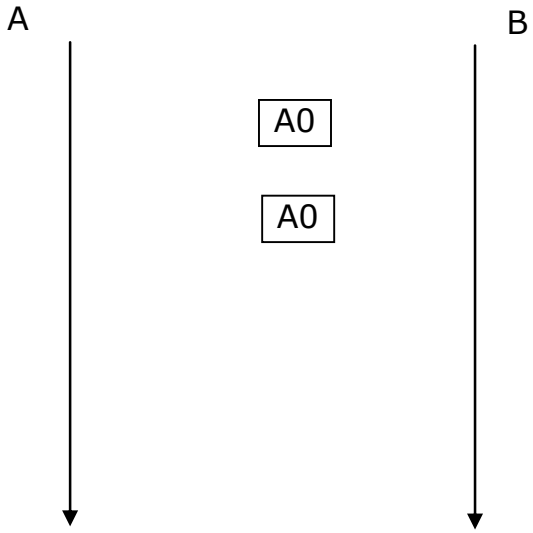
Aucune perte :



Le premier message A0 est perdu :







4.2. Quelle est la stratégie adoptée par A pour fermer la connexion ? (0,5 point)

4.3. Montrer que ce protocole satisfait la propriété P1 (**B a la certitude que A va fermer la connexion**) avec la probabilité $Q=1-p^N$. (0,5 point)

4.4. A en déduit que B connaît son intention de fermer la connexion avec la probabilité Q. Est-ce que la propriété P2 (**A a la certitude que B a la certitude que A va fermer la connexion**) peut être vérifiée avec une probabilité de 1 ? (0,5 point)

4.5. Est-ce que A peut être bloqué, et avec quelle probabilité ? (0,5 point)

4.6. B peut recevoir des messages de données ou un message de fermeture de connexion. Du point de vue de B, peut-il rester bloquer si A décide de fermer la connexion ? Avec quelle probabilité peut-il rester bloquer ? En déduire la probabilité pour que P3 (**Ni A ni B ne restent bloqués en attente de message**) soit vérifiée. (0,5 point)

Question 5 : (3 points)
Toutes les variables et constantes dans les algorithmes sont des entiers, quand ce n'est pas le cas, le type est donné.

On construit une solution sur la base suivante.

Soit le comportement de A :

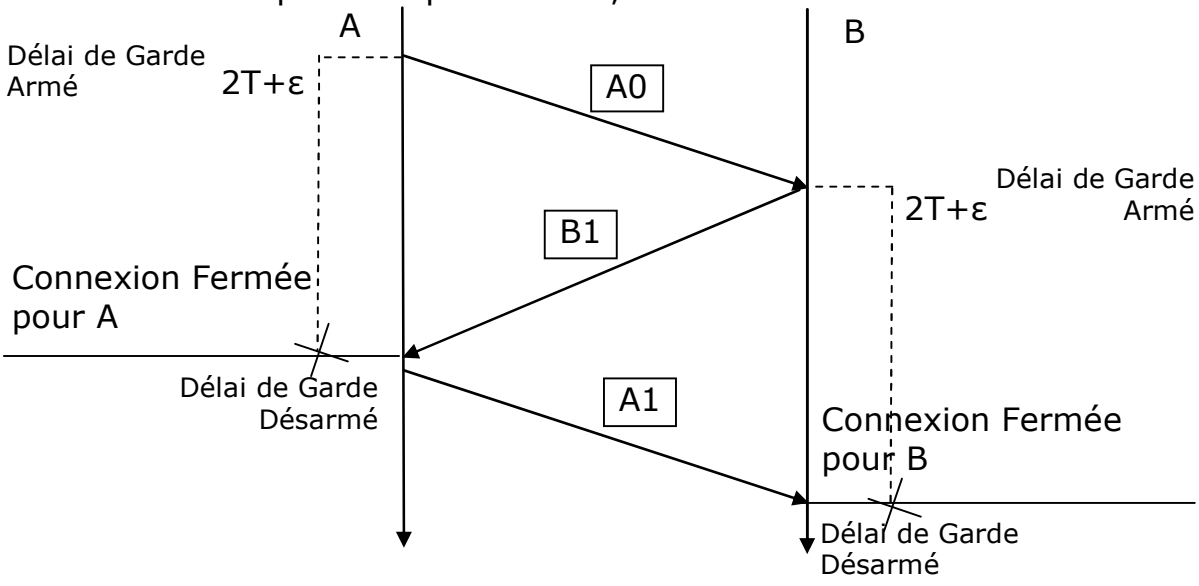
```
Début
Constante N;
K := 1 ;
Bouléen Fini := faux;
Evénement E ;
Répéter
     Envoyer A0;
     Armer (DélaiDeGarde, 2T+ε);
     Attendre (E);
     Si (E == message B1)
          Alors
               Fini := vrai;
               Désarmer (DélaiDeGarde);
               Envoyer A1;
          Sinon
               Si (K == N) Alors Fini := Vrai Sinon K := K + 1 Finsi
     Finsi
Jusqu'à Fini
Fermer la connexion;
Fin
```

Soit le comportement de B :

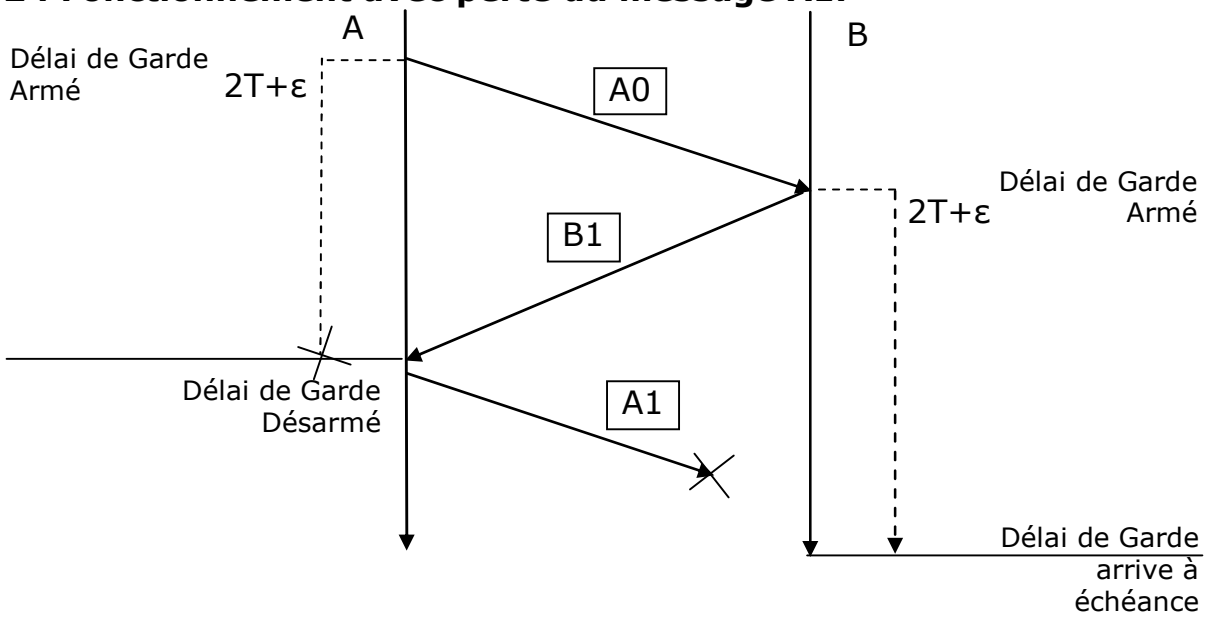
```
Début
Constante N;
K := 1 ;
Bouléen Fini := faux;
Evénement E;
Attendre E;
Si (E == message A0)
     Alors
          Répéter
               Envoyer B1
               Armer (DélaiDeGarde, 2T+ε);
               Attendre (E);
               Si (E == message A1)
                    Alors
                        Fini := vrai;
                        Désarmer (DélaiDeGarde);
                    Sinon
                        Si (K == N)
                           Alors Fini := Vrai
                           Sinon K := K + 1
                        Finsi
               Finsi
          Jusqu'à Fini
          Fermer la connexion
     Sinon
          Recevoir Message
Finsi;
Fin
```

5.1 N=1 pour toute la question 5.
Compléter les scénarii qui suivent en faisant fonctionner le protocole spécifié ci-dessus et en donnant à chaque fois l'état de la connexion pour A et pour B. Commenter votre solution si nécessaire. (1,5 points)

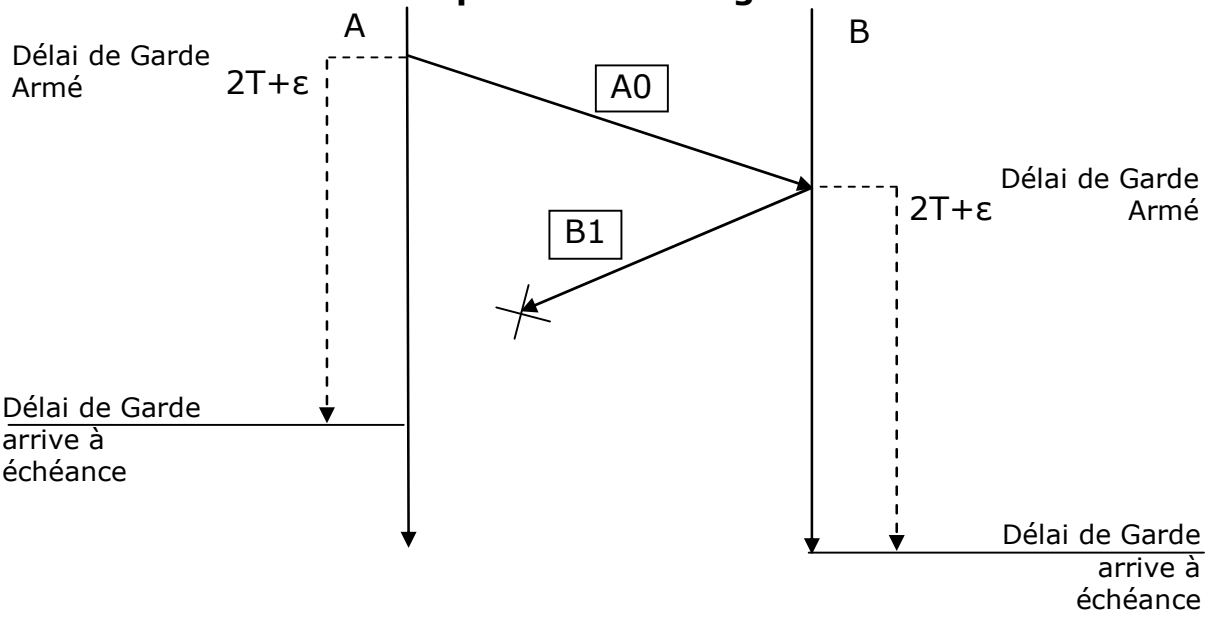
Cas 1 : Fonctionnement sans perte de message. Après Réception de B1, A ferme la connexion. Après réception de A1, B ferme la connexion.



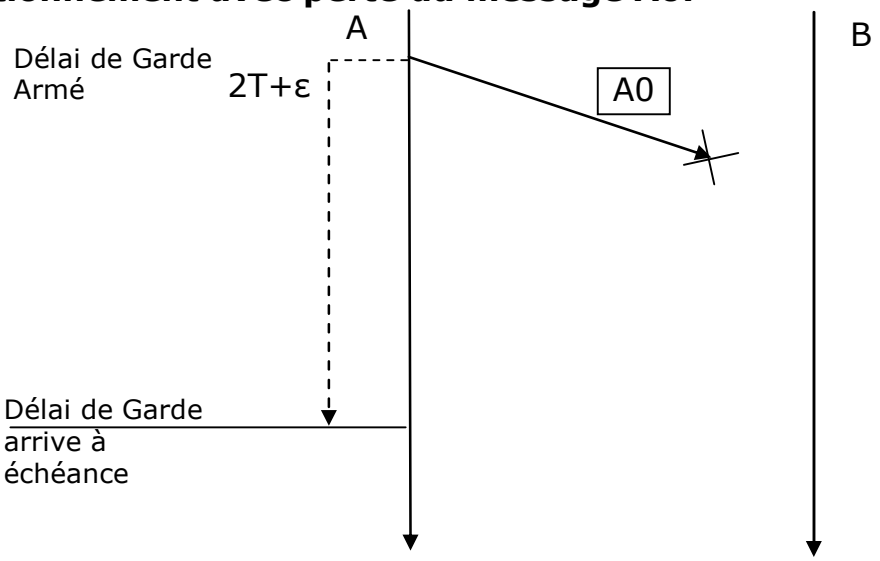
Cas 2 : Fonctionnement avec perte du message A1.



Cas 3 : Fonctionnement avec perte du message B1.



Cas 4 : Fonctionnement avec perte du message A0.



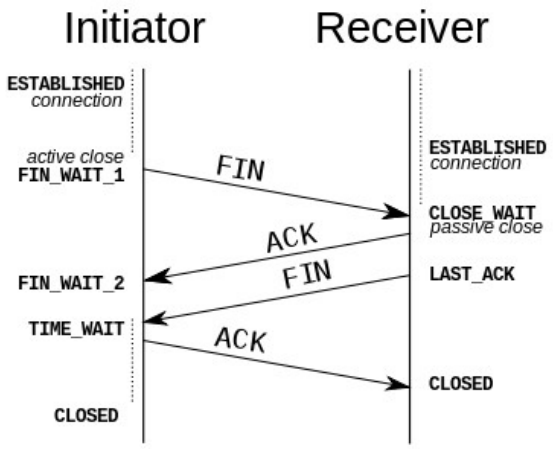
Soit p la probabilité qu'un message soit perdu.

5.2. Avec N=1, quelle est la probabilité que la propriété P1 (**B a la certitude que A va fermer la connexion**) soit vérifiée ? (0,5 point)

5.3. Avec N=1, quelle est la probabilité que la propriété P2 (**A a la certitude que B a la certitude que A va fermer la connexion**) soit vérifiée ? Pour vous aider, penser à la probabilité de l'événement contraire. (0,5 point)

5.4. Avec N=1, dans le cas 4, quelle est la probabilité que la propriété P3 (**Ni A ni B ne restent bloqués en attente de message**) soit vérifiée ? (0,5 point)

Question 6 : (3 points)
TCP (Transmission Control Protocol) de l'Internet effectue la fermeture de connexion comme indiqué dans le dessin ci-dessous :

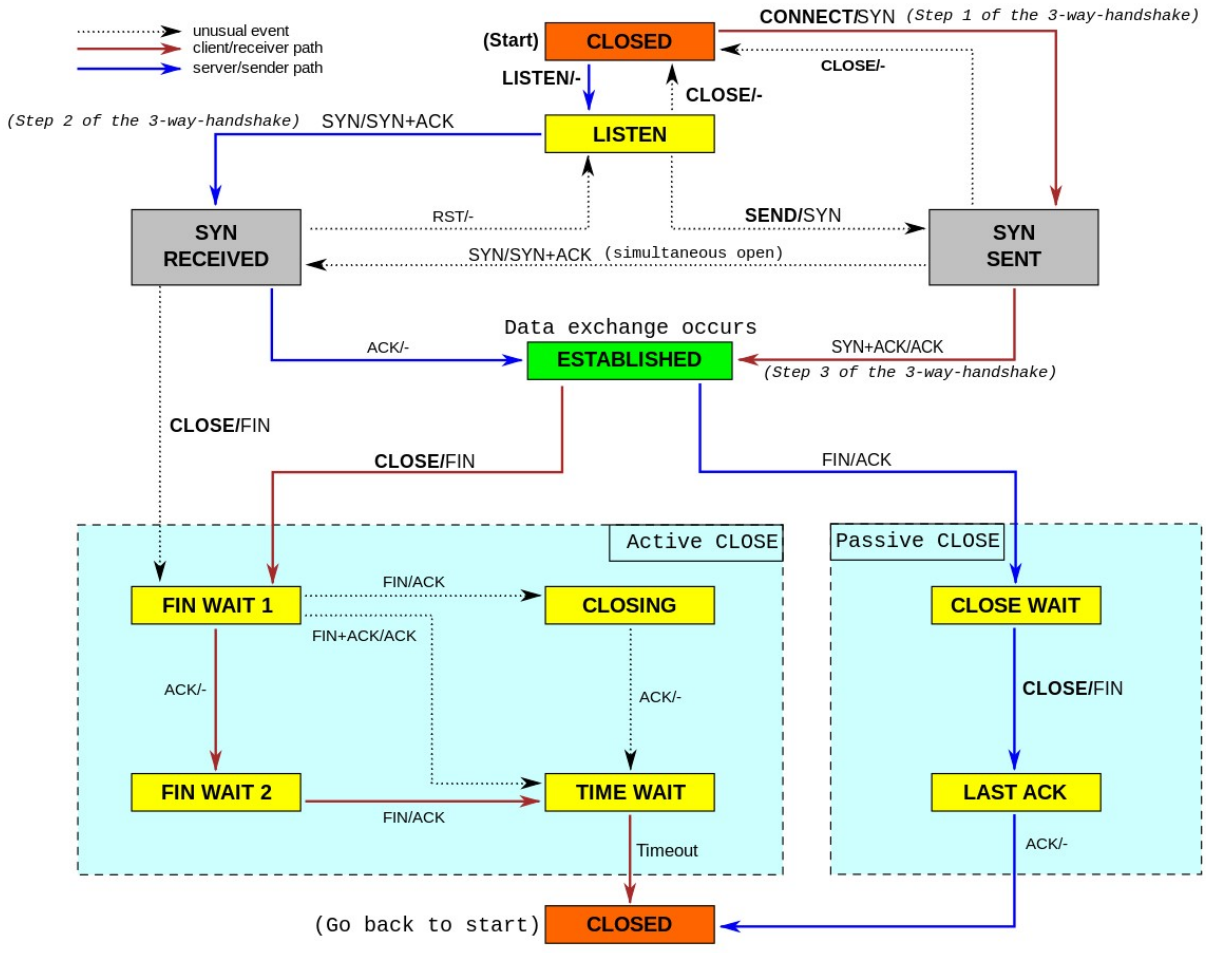


Source https://en.wikipedia.org/wiki/Transmission_Control_Protocol, consulté le 05/08/2020.

On peut combiner le ACK et le FIN des échanges du milieu dans un seul message (segment TCP). On passe alors d'un 4-way handshake[4] à un 3-way handshake.

Il est précisé que si le segment initial FIN est perdu, il est réémis après l'écoulement d'un délai de garde (TIMEOUT). Et plus généralement les mécanismes de transmission fiable s'appliquent.

On vous donne aussi l'automate à états du protocole TCP mais c'est surtout la partie fermeture de connexion dans le bas qui vous concerne:



[4] En réalité, ce serait plutôt deux 2-way handshakes. Tel qu'il est conçu TCP ferme la connexion dans chaque sens séparément mais il y a bien un initiateur de la fermeture de connexion.

La source a été consultée le 24/08/2020 : https://en.wikipedia.org/wiki/Transmission_Control_Protocol#/media/File:Tcp_state_diagram_fixed_new.svg

L'interprétation des étiquettes sur les arcs entre les états est la suivante :
"occurrence d'un événement ou d'une condition à vraie/action".

Par exemple : FIN/ACK s'interprète comme "si un FIN est reçu, on envoie un ACK".

En vous aidant de la question 5, est-ce que P1, P2, P3 sont vérifiées ? Quelle serait la valeur de N pour TCP ? Est-ce que P4 est vérifiée ? (1 point)

Question 7 : Optionnelle, rapporte des points en plus, mais vous pouvez la sauter. (3 points)
Cette question rend l'examen sur 23 points au total.

Maintenant, N est strictement supérieur à 1. Donc on émet potentiellement plusieurs fois le même message de fin : A1 ou B1.

On considère toujours p comme la probabilité de perdre un message.

7.1. Quelle est la probabilité que P1 soit vérifiée ? (0,5 point)

7.2. Quelle est la probabilité que P2 soit vérifiée ? (0,5 point)

7.3. Quelle est la probabilité que P3 soit vérifiée ? (0,5 point)

7.4. Si N tend vers l'infini (N-> $+\infty$) montrer que les propriétés P1, P2, P3 sont vérifiées avec une probabilité égale à 1. (0,5 point)

7.5. Si N tend vers l'infini (N-> $+\infty$) qu'en est-il de la propriété 4 ? On rappelle que l'ensemble des entiers naturels $\mathbb{N}$ est un ensemble infini dénombrable. (1 point)
Le cardinal de $\mathbb{N}$ est le plus petit cardinal infini, il est noté $\aleph_0$.