



Année universitaire 2019-2020

## **SUJET RSX101 : Réseaux et Protocoles pour l'Internet**

Examen 1<sup>e</sup> session du 27/01/2020

Responsable : E. GRESSION-SOUDAN

Durée : 3 heures

### **Consignes**

Calculatrice autorisée sur un équipement différent du téléphone mobile.

Tous documents autorisés

**Les téléphones mobiles sont interdits  
autres équipements communicants autorisés mais Internet interdit.**

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 20 points

Sujet avec correction de **25 pages**, celle-ci comprise.

**Le corrigé est bien plus détaillé que les réponses qui étaient demandées à l'examen... c'est un dernier exercice ;-)**

**Important :** Les étudiants répondent sur les feuilles du sujet d'examen, et si nécessaire complètent leur réponse sur une copie double en faisant référence à quelle question correspond quelle réponse.

**Bien mettre le numéro des questions avec leurs réponses sur la copie.**

Vous rendrez une copie double au moins afin de donner les informations d'usage (nom, prénom...) et de récupérer un numéro de copie que vous ajouterez sur les feuilles du sujet d'examen. La copie doit être remise aux surveillants avec le coin cacheté.

→ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

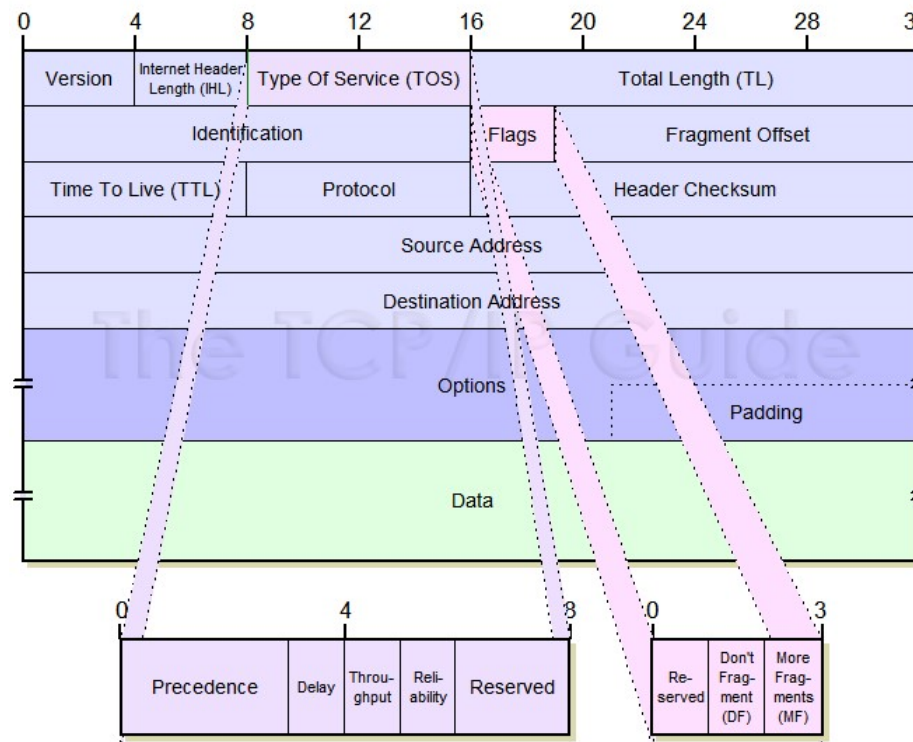
**1/25**

## Exercice 1 : Découverte d'un Protocole de Transport (10 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](http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm) :



On s'intéresse à une capture Wireshark qui concerne un protocole que vous ne connaissez pas : DCCP (Datagram Congestion Control Protocol).

### Question 1 : On s'intéresse en particulier à la trame 1 pour l'instant. (4 points)

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Request] Seq=38464816766 (service code)
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
✓ Ethernet II, Src: Intel_bd:5d:1f (00:07:e9:bd:5d:1f), Dst: Dell_59:55:51 (00:14:22:59:55:51)						
> Destination: Dell_59:55:51 (00:14:22:59:55:51)						
> Source: Intel_bd:5d:1f (00:07:e9:bd:5d:1f)						
Type: IPv4 (0x0800)						
✓ Internet Protocol Version 4, Src: 139.133.209.176, Dst: 139.133.209.65						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 52						
Identification: 0xff20 (65312)						
> Flags: 0x4000, Don't fragment						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 64						
Protocol: Datagram Congestion Control Protocol (33)						
Header checksum: 0x818b [validation disabled]						
[Header checksum status: Unverified]						
Source: 139.133.209.176						
Destination: 139.133.209.65						
✓ Datagram Congestion Control Protocol, Src Port: 39420, Dst Port: 5001 [Request] Seq=38464816766						
Source Port: 39420						
Destination Port: 5001						
Data Offset: 8						
CCVal: 0						
Checksum Coverage: 0						
Checksum: 0xaaaf3 [correct]						
[Checksum Status: Good]						
Type: Request (0)						
Extended Sequence Numbers: True						
Sequence Number: 38464816766						
Service Code: 0						
> Options: (12 bytes)						
0000	00 14 22	59 55 51 00 07	e9 bd 5d 1f 08 00 45 00	..YUQ.. ..]	...E-	
0010	00 34 ff	20 40 00 40 21	81 8b 8b 85 d1 b0 8b 85	-4- @-@!	.....	
0020	d1 41 99	fc 13 89 08 00	aa f3 01 00 00 08 f4 ae	-A-.....	.....	
0030	86 7e 00	00 00 00 20 04	05 02 22 04 01 02 20 04	~.....	.."	
0040	01 02			..		

- Délimiter l'entête de la trame Ethernet dans la capture en hexadécimal ci-dessous. **(0,25 point)**
- Délimiter l'entête du datagramme IP dans la capture en hexadécimal ci-dessous. **(0,25 point)**
- Délimiter le datagramme DCCP dans la capture en hexadécimal ci-dessous. **(0,25 point)**
- Est-ce que DCCP est un protocole de transport, de session, de présentation ou d'application ? **(0,25 point)**

Ne pas hésiter à utiliser des couleurs différentes pour que votre réponse soit facile à lire.

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

0000      00 14 22 59 55 51 00 07      e9 bd 5d 1f 08 00      45 00  
            entête Ethernet

0010      00 34 ff 20 40 00 40 21      81 8b 8b 85 d1 b0 8b 85

entête IP, 20 octets, car "5" dans le champ longueur de l'entête, donc  $5 \times 4 = 20$  octets d'entête (pas d'options)  
longueur du datagramme 34 en hexadécimal ou 52 en décimal : entête et charge utile, cette information peut nous dire si Wireshark affiche le FCS ou pas de la trame Ethernet... on connaît la réponse à travers les exercices, mais ici on peut vérifier que la fin du datagramme tombe avec le dernier octet affiché, donc comme le sait, le champ FCS n'est pas affiché, de toute façon il vaudrait 0 car la trame a bien été reçue par Wireshark

0020      d1 41 99 fc 13 89 08 00      aa f3 01 00 00 08 f4 ae  
            entête DCCP, on la calcule à partir des champs détaillés dans la trace Wireshark

on a :

- 2 numéros de port 99 fc 13 89: 2 + 2 octets,
- checksum 4 octets, bien identifiables dans l'entête commenté, aaf3, donc ce qui entre les deux correspond à des champs de l'entête soit : "DataOffset", "CCval", et "Checksum coverage" soit un total de 2 octets : 08 00 au passage, on retrouve bien 08 pour le Data Offset, qui nous dit qu'il y a des données a priori à la fin de la partie DCCP.
- un numéro de séquence TCP est sur 32 bits (4 octets) on peut supposer qu'un numéro de séquence étendu est sur 64 bits soit 8 octets sinon sur 6 octets ? avant on doit avoir un champ type requête, puis un indicateur qui dit si on est en numérotation étendue ou pas, cela pourrait correspondre à "01" ?
- après le numéro de séquence vaut 38 464 816 766 en décimal (pas une seule lettre dedans donc ce n'est pas de l'hexadécimal, il y a un 8 ce n'est pas de l'octal non plus) d'après la trace commencée, si on convertit ce

→ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

chiffre en hexadécimal cela donne : 8 F4AE 867E qui est plus long que 4 octets et qu'on retrouve dans la partie DCCP.

6 ou 8 octets ? un nombre impaire d'octets est peu pensable car c'est inefficace en terme de calcul et d'extraction de champ d'entête, les champs doivent être sur des frontières de mot machine, ou de demi mot.

8 octets, on englobe le 01 des champs requête & indicateur, donc c'est plutôt 6 octets

0030    86 7e   00 00 00 00 20 04    05 02 22 04 01 02 20 04  
         service code                    champ options ?

0040    01 02  
         fin du champ option ou données ?

- on a un type "service code" qui vaut 0. Il est sur 1, 2 ou 4 octets. 1 octet c'est plutôt improbable, une intuition car ça ne me semble pas s'aligner avec les frontières de mots ou de demi-mots.
  1. On essaie 4 octets on a alors pour les options : 20 04 05 02 22 04 01 02 20 04 01 02, mais pas de données
  2. On essaie 2 octets on a alors pour les options : 00 00 20 04 05 02 22 04 01 02 20 04 mais pas 2 octets de données

Il reste à faire qqch du "Data Offset" = "8" ? ce n'est pas une longueur en octets car quand on compte à partir du premier octet de l'entête on tombe dans un de ses champs. Faisons l'hypothèse qu'il faut le multiplier par 4 octets comme dans l'entête d'IP avec le champ longueur de l'entête... dans ce cas, on trouve 32, qui nous mène juste après le 01 02 final, ça fait sens mais il n'y a pas de données...

Je ne vois pas d'autre proposition qui ferait sens ? Ca serait donc le cas 1 qui collerait le mieux ?

Regardons ce qu'on obtient en utilisant l'outil wireshark. La zone en bleu dans la partie hexadécimale correspond à l'entête DCCP. C'est l'option 1 qui est la bonne et donc le service code est sur 4 octets et vaut "0000".



- ▼ Datagram Congestion Control Protocol, Src Port: 39420, Dst Port: 5001 [Reque
  - Source Port: 39420
  - Destination Port: 5001
  - Data Offset: 8
  - CCVal: 0
  - Checksum Coverage: 0
  - Checksum: 0xaaf3 [correct]
  - [Checksum Status: Good]
  - Type: Request (0)
  - Extended Sequence Numbers: True
  - Sequence Number: 38464816766
  - Service Code: 0
- ▼ Options: (12 bytes)
  - > Option Type: Change L (32)
  - > Option Type: Change R (34)
  - > Option Type: Change L (32)

---

0000 00 14 22 50 55 51 00 07 00 6d 5d 1f 00 00 15 00 "VUO 1 E

Pour répondre, on peut aussi faire un coup de bluff. C'est une première trame qui initie une mise en relation, elle est vraisemblablement courte donc, il est possible qu'il n'y ait pas de données. On peut se dire que l'entête DCCP va jusqu'à la fin de la charge utile de la trame Ethernet... Sachant que l'entête DCCP n'est pas donnée, on peut se dire aussi que la réponse devrait être simple.

Pour finir de répondre à la question, DCCP est très probablement un protocole de transport (couche 4), donc une alternative à TCP et UDP. Il est directement au-dessus de IP. Il utilise comme TCP et UDP des numéros de port pour identifier les applications communicantes au-dessus d'IP.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

L'entête DCCP est la suivante, version numéro de séquence long et numéro de séquence court, issue de la RFC4340 qui décrit DCCP :

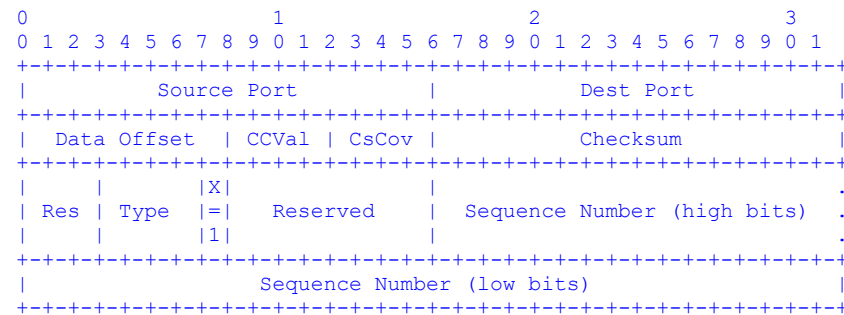


Figure 2: The extended DCCP Header with Long Sequence Numbers [RFC4340]

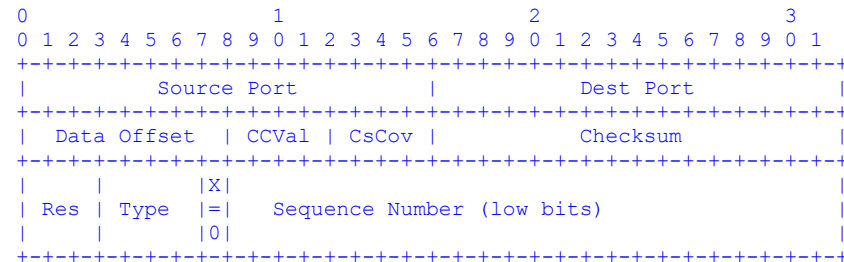
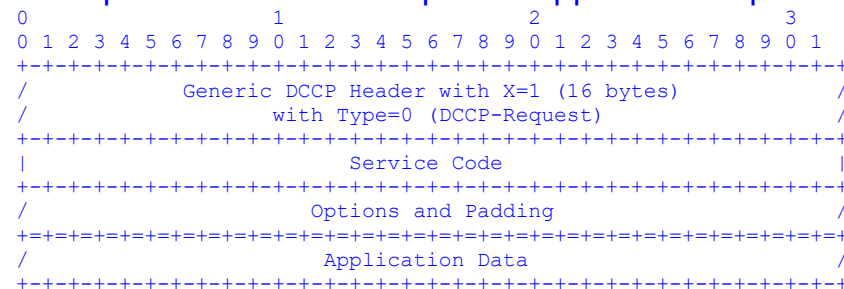


Figure 3: The short DCCP Header with Short Sequence Numbers [RFC4340]

Dans la trame que nous examinons, X vaut 1 (3<sup>ème</sup> ligne champs Request et Extended Sequence Numbers : true, "01") ce qui confirme que les numéros de séquence sont sur 6 octets.

Une vision plus méta de l'entête, DCCP-Request Packets mais qui fait apparaître la partie option :



➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

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

- Quelle est l'adresse Ethernet destination en **hexadécimal** ? (0,25 point) 00 14 22 59 55 51
- Quelle est l'adresse Ethernet source en **hexadécimal** ? (0,25 point) 00 07 e9 bd 5d 1f
- Quel est le type de la trame en **hexadécimal** ? (0,25 point) 08 00
- Quelle est la version du protocole IP en **décimal** ? (0,25 point) 4 version 4
- Quelle est la longueur de l'entête IP en **décimal** ? (0,25 point) 5  $5 * 4 = 20$  octets
- Quelle est l'adresse IP source en **hexadécimal** ? (0,25 point) 8b 85 d1 b0
- Quelle est l'adresse IP destination en **hexadécimal** ? (0,25 point) 8b 85 d1 41
- Quel est le numéro du protocole indiqué par l'entête IP associé à DCCP en **hexadécimal** ? (0,25 point) 21 soit 33
- Quelle est la longueur totale du datagramme en **décimal** ? (0,25 point) 00 34 soit 52 en décimal
- Quel est le numéro de port source en **hexadécimal** ? (0,25 point) 99 fc soit 39420
- Quel est le numéro de port destination en **hexadécimal** ? (0,25 point) 13 89 soit 5001
- Quel est le numéro de séquence inclu dans l'entête DCCP en **hexadécimal** ? (0,25 point) 00 08 f4 ae 86 7e



**Question 2 :** On vous donne la totalité de l'échange. **(4 points)**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Request] Seq=38464816766 (service=0)
2	0.000374	139.133.209.65	139.133.209.176	DCCP	82	5001 → 39420 [Response] Seq=1960341146 (Ack=38464816766) (service=0)
3	0.000493	139.133.209.176	139.133.209.65	DCCP	70	39420 → 5001 [Ack] Seq=38464816767 (Ack=1960341146)
4	0.012982	139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)
5	0.013513	139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341147 (Ack=38464816768)
6	0.014428	139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816769 (Ack=1960341147)
7	0.014789	139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341148 (Ack=38464816769)
8	0.015423	139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816770 (Ack=1960341148)
9	0.015490	139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816771 (Ack=1960341148)
...	0.015871	139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341149 (Ack=38464816770)
...	0.016080	139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341150 (Ack=38464816771)
...	0.016420	139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816772 (Ack=1960341150)
...	0.016494	139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Close] Seq=38464816773 (Ack=1960341150)
...	0.016899	139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341151 (Ack=38464816772)
...	0.017270	139.133.209.65	139.133.209.176	DCCP	74	5001 → 39420 [Reset] Seq=1960341152 (Ack=38464816773) (code=Closed)

- A partir de cette trace, et uniquement celle-ci, indiquer les apparentes similitudes entre DCCP et les deux protocoles bien connus : TCP et UDP. **(1 point)**

**Correction :**

- UDP est non fiable (pas d'acquittement), dans DCCP il y en a.
- Par son nom, on sait que DCCP est un protocole à Datagramme. Donc, on peut faire l'hypothèse qu'il n'est pas orienté flot d'octets comme l'est TCP.
- Généralement Datagramme rime avec non fiable... mais ici on voit bien que des acquittements circulent. Pourrait-on alors conclure que DCCP est un protocole de transport orienté messages quasiment fiable ? Difficile d'en dire plus.
- Dans le nom, on a "Congestion Control", on est en droit de supposer que d'une façon ou d'une autre, DCCP incorpore un contrôle de congestion comme TCP ou un autre. En tous cas, ce n'est pas facile à voir dans la trace.
- Rien ne fait mention d'un contrôle de flux. Rien ne fait mention d'une délivrance des messages dans l'ordre à l'application.

On peut faire un tableau récapitulatif.

Propriétés	UDP	TCP	DCCP
Couche transport	Oui	Oui	Oui
fiable	Non	Oui	Probablement oui, à cause des acquittements
piggybacking	-	Oui	Oui
association/connexion	Non, enfin juste pour désigner	Oui	Plutôt oui
Contrôle de congestion	Non	Oui	A priori oui
TCP friendly	Non		Objectif à atteindre
orienté	Messages	Octets	Messages
Contrôle de flux	Non	Oui	Non
Livraison à l'application	Best effort	En séquence	?
Protocole à Etats	Non	Oui	?

- Est-ce que la notion d'extrémité est conservée avec DCCP ? Si oui, donner les extrémités associées à l'échange. **(0,5 point)**

**Correction :**

En effet, la notion d'extrémité qu'on a avec TCP et qui est étendue à UDP se retrouve ici. L'extrémité source est <139.133.209.176, 39420>. L'extrémité destination source est <139.133.209.65, 5001>.

- Est-ce que le protocole numérote les octets ou les messages d'après vos observations ? Pourquoi selon vous ? **(0,5 point)**

Pour compléter votre analyse de la trace ci-dessus et vous aider on vous donne l'analyse Wireshark de la trame 4.

**Correction :**

A la trame 1, le numéro de séquence DCCP de <139.133.209.176, 39420> vers <139.133.209.65, 5001> vaut 38 464 816 766. On sait qu'il n'y a pas de données dans ce datagramme DCCP.

Dans la trame 2 qui va en sens inverse, l'ack porte le numéro 38 464 816 766. Donc on n'a rien acquitté.

Dans la trame 3 [Ack], de <139.133.209.176, 39420> vers <139.133.209.65, 5001> le numéro de séquence DCCP vaut 38 464 816 767.

Dans la trame 4 [DataAck] dans le même sens que la trame 3, le numéro de séquence DCCP vaut 38 464 816 768. Il y a 96 octets de données dans ce datagramme.

Des trames 1, 3 et 4, on pourrait faire l'hypothèse que DCCP acquitte vraiment les messages, tous les messages quel que soit leur type, et pas les octets. Ca se confirmerait avec la trame 6.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

Un autre argument : comme on est dans un protocole orienté message, ça n'a pas de sens d'acquitter à l'échelle des octets.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.012982	139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)

> Frame 4: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits)

> Ethernet II, Src: Intel\_bd:5d:1f (00:07:e9:bd:5d:1f), Dst: Dell\_59:55:51 (00:14:22:59:55:51)

> Internet Protocol Version 4, Src: 139.133.209.176, Dst: 139.133.209.65

✓ Datagram Congestion Control Protocol, Src Port: 39420, Dst Port: 5001 [DataAck] Seq=38464816768

Source Port: 39420

Destination Port: 5001

Data Offset: 9

CCVal: 0

Checksum Coverage: 6

Checksum: 0x7d28 [correct]

[Checksum Status: Good]

Type: DataAck (4)

Extended Sequence Numbers: True

Sequence Number: 38464816768

Acknowledgement Number: 1960341146

> Options: (12 bytes)

✓ Data (96 bytes)

Data: 202122232425262728292a2b2c2d2e2f3031323334353637...

[Length: 96]

On observe les échanges de la trace ci-dessus, les numéros de séquences et les numéros d'acquittement qui circulent dans les datagrammes DCCP. Est-ce qu'un Ack acquitte plusieurs Datagrammes DCCP dans la trace comme dans TCP ? **(0,5 point)**

Attention, dans DCCP, un datagramme peut n'inclure qu'un Ack, donc aucune donnée. Le type DataAck, c'est quand il y a des données et un Ack.

### Correction :

Les acquittements acquittent le dernier message reçu, et pas le prochain message à recevoir, c'est une logique différente de TCP qui acquitte en envoyant le numéro du prochain octet à recevoir. C'est une différence entre DCCP et TCP qu'on ne pouvait observer pour la première interrogation de la question 2.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

11/25



Ce qu'on observe, c'est que les numéros de séquence des datagrammes DCCP envoyés par <139.133.209.176, 39420> ne s'incrémentent que d'une unité à chaque fois, [Ack] comme [DataAck], et les acquittements correspondants issus de <139.133.209.65, 5001> n'acquittent que des numéros qui portent sur les [DataAck] globalement. Dans cette observation, on ne considère pas la mise en relation et la fin de relation.

Est-ce qu'on doit considérer cela comme un acquittement groupé ? On n'a pas assez de données d'observation pour avoir une conclusion bien claire. Mais en général, les messages sont acquittés un par un, sauf la trame 5 (Ack =38464816768) issue du serveur qui acquitte les trames 3 (Seq=38464816767) et 4 (Seq=38464816768) issues du client.

Commenter la nature des échanges ci-dessous : mise en relation, échange de données, acquittement... Vous pouvez répondre sur la trace directement. **(1,5 points)**

Source	Destination	Protoco	Length	Info
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Request] Seq=38464816766 (service=0)
139.133.209.65	139.133.209.176	DCCP	82	5001 → 39420 [Response] Seq=1960341146 (Ack=38464816766) (service=0)
139.133.209.176	139.133.209.65	DCCP	70	39420 → 5001 [Ack] Seq=38464816767 (Ack=1960341146)
139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341147 (Ack=38464816768)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816769 (Ack=1960341147)
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341148 (Ack=38464816769)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816770 (Ack=1960341148)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816771 (Ack=1960341148)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341149 (Ack=38464816770)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341150 (Ack=38464816771)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816772 (Ack=1960341150)
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Close] Seq=38464816773 (Ack=1960341150)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341151 (Ack=38464816772)
139.133.209.65	139.133.209.176	DCCP	74	5001 → 39420 [Reset] Seq=1960341152 (Ack=38464816773) (code=Closed)

**Correction :**

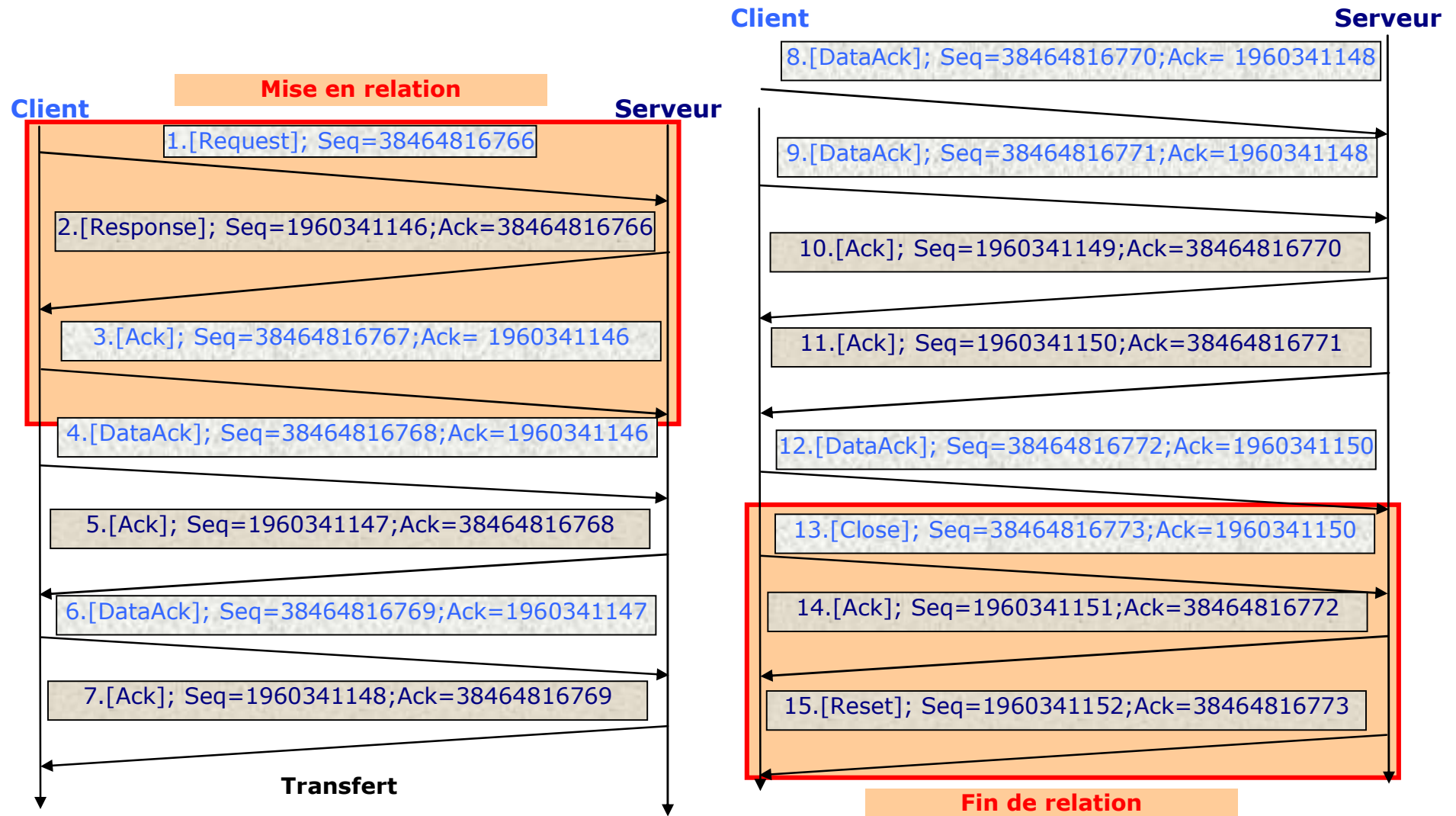
Source	Destination	Protoco	Length	Info	Mise en relation
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Request] Seq=38464816766 (service=0)	<b>Transfert de données</b>
139.133.209.65	139.133.209.176	DCCP	82	5001 → 39420 [Response] Seq=1960341146 (Ack=38464816766) (service=0)	
139.133.209.176	139.133.209.65	DCCP	70	39420 → 5001 [Ack] Seq=38464816767 (Ack=1960341146)	
139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)	
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341147 (Ack=38464816768)	
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816769 (Ack=1960341147)	
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341148 (Ack=38464816769)	
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816770 (Ack=1960341148)	
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816771 (Ack=1960341148)	
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341149 (Ack=38464816770)	
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341150 (Ack=38464816771)	
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816772 (Ack=1960341150)	
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Close] Seq=38464816773 (Ack=1960341150)	
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341151 (Ack=38464816772)	
139.133.209.65	139.133.209.176	DCCP	74	5001 → 39420 [Reset] Seq=1960341152 (Ack=38464816773) (code=Closed)	

**Fin de relation**

On observe 3 phases. On peut donc les baptiser en "phase de mise en relation" avec Request-Response-Ack, "phase de transfert de données" avec DataAck-Ack, "phase de fin de relation" avec Close-Ack-Reset.



Pour aller plus loin, on peut faire un diagramme d'enchaînement des datagrammes DCCP :

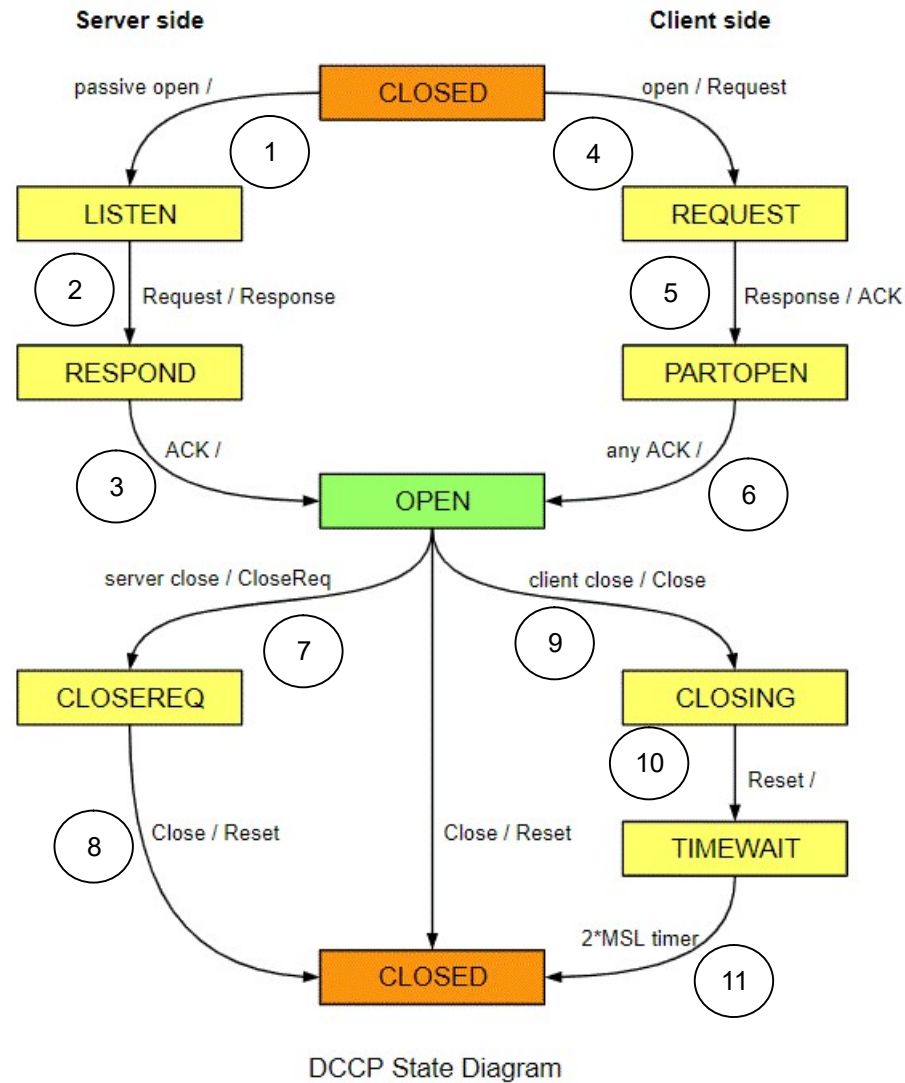


→ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :



**Question 3 :** On vous donne le diagramme d'états de l'automate protocolaire DCCP. Ajouter les transitions de l'automate sur la trace ci-dessous ainsi que les états pour chacune des entités communicantes ? En déduire quelle est l'adresse IP et le numéro de port du serveur dans la trace. **(2 points)**



➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

15/25

Source	Destination	Protoco	Length	Info
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Request] Seq=38464816766 (service=0)
139.133.209.65	139.133.209.176	DCCP	82	5001 → 39420 [Response] Seq=1960341146 (Ack=38464816766) (service=0)
139.133.209.176	139.133.209.65	DCCP	70	39420 → 5001 [Ack] Seq=38464816767 (Ack=1960341146)
139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341147 (Ack=38464816768)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816769 (Ack=1960341147)
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341148 (Ack=38464816769)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816770 (Ack=1960341148)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816771 (Ack=1960341148)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341149 (Ack=38464816770)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341150 (Ack=38464816771)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816772 (Ack=1960341150)
139.133.209.176	139.133.209.65	DCCP	66	39420 → 5001 [Close] Seq=38464816773 (Ack=1960341150)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341151 (Ack=38464816772)
139.133.209.65	139.133.209.176	DCCP	74	5001 → 39420 [Reset] Seq=1960341152 (Ack=38464816773) (code=Closed)

Client state

CLOSED

Server state

LISTEN

Correction

Source	Destination	Protoco	Length	Info
REQUEST	139.133.209.176	139.133.209.65	DCCP	66 39420 → 5001 [Request] Seq=38464816766 (service=0)
139.133.209.65	139.133.209.176	DCCP	82	5001 → 39420 [Response] Seq=1960341146 (Ack=38464816766) (service=0)
PART OPEN	139.133.209.176	139.133.209.65	DCCP	70 39420 → 5001 [Ack] Seq=38464816767 (Ack=1960341146)
139.133.209.176	139.133.209.65	DCCP	166	39420 → 5001 [DataAck] Seq=38464816768 (Ack=1960341146)
OPEN	139.133.209.65	139.133.209.176	DCCP	66 5001 → 39420 [Ack] Seq=1960341147 (Ack=38464816768)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816769 (Ack=1960341147)
139.133.209.65	139.133.209.176	DCCP	66	5001 → 39420 [Ack] Seq=1960341148 (Ack=38464816769)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816770 (Ack=1960341148)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816771 (Ack=1960341148)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341149 (Ack=38464816770)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341150 (Ack=38464816771)
139.133.209.176	139.133.209.65	DCCP	162	39420 → 5001 [DataAck] Seq=38464816772 (Ack=1960341150)
CLOSING	139.133.209.176	139.133.209.65	DCCP	66 39420 → 5001 [Close] Seq=38464816773 (Ack=1960341150)
139.133.209.65	139.133.209.176	DCCP	70	5001 → 39420 [Ack] Seq=1960341151 (Ack=38464816772)
TIME WAIT	139.133.209.65	139.133.209.176	DCCP	74 5001 → 39420 [Reset] Seq=1960341152 (Ack=38464816773) (code=Closed)

CLOSED

CLOSED

→ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

16/25

On peut aussi tenter de représenter les changements d'état dans un tableau, c'est plus long mais plus précis.

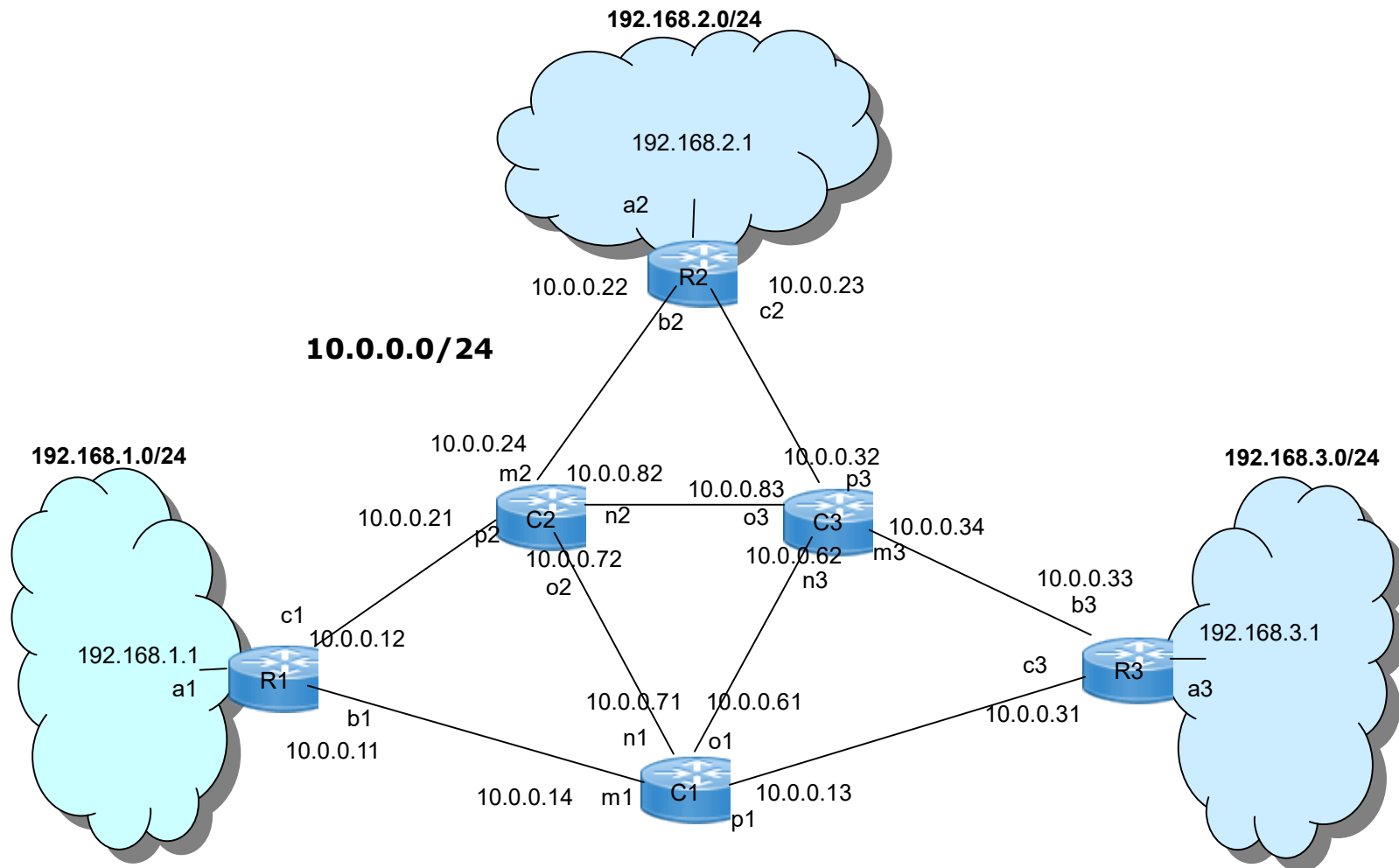
Client - <139.133.209.176,39420>			Type	Sens	<139.133.209.65, 5001> - Serveur		
Trame	Etat Client	Transition			Transition	Etat Serveur	Trame
						CLOSED	
			passive open()		①	LISTEN	
	CLOSED						
1	REQUEST	④	open() Request	➔	②	RESPOND	
	PARTOPEN	⑤	Response	←			2
3	OPEN	⑥	Ack	➔	③	OPEN	
4	OPEN		DataAck	➔		OPEN	
			Ack	←			5
6			DataAck	➔			
			Ack	←			7
8			DataAck	➔			
9			DataAck	➔			
			Ack	←			10
			Ack	←			11
12	OPEN		DataAck	➔		OPEN	
13	CLOSING	⑨	Close	➔	⑦	CLOSEREQ	
			Ack	←			14 <sup>1</sup>
	TIMEWAIT	⑩	Reset	←	⑧	CLOSED	15
		2*MSL					
	CLOSED	11					

<sup>1</sup> La trame 14 doit être liée à la 12... c'est l'hypothèse qui semble la plus raisonnable car "Ack" n'apparaît pas dans l'automate protocolaire DCCP.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

## Exercice 2 : Routage OSPF et Multicast IP (10 points)

Soit le réseau IP ci-dessous :



Toutes les interfaces d'un routeur sont identifiées : ai, bi, ci pour un routeur feuille Ri, et mi, ni, oi, pi pour un routeur de cœur Ci (i=1 à 3). Le réseau cœur a une adresse 10.0.0.0/24. Les réseaux feuilles ont respectivement les adresses 192.168.1.0/24, 192.168.2.0/24 et 192.168.3.0/24. Le découpage en sous-réseaux de ces réseaux feuilles n'est pas dans le sujet de l'examen.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

18/25



**Question 1 (1,5 points) :** C1 est le routeur par défaut de R1. R1 ne cherche à atteindre que des réseaux feuilles qui correspondent à ses utilisateurs et ses serveurs. Dans l'hypothèse d'un routage statique, donner la table de routage de R1. Dans la table de routage, on fait figurer une colonne réseau destination et le masque au format compact, puis l'interface de sortie, et l'adresse IP du prochain routeur, le type (DIRECT ou DISTANT).

**Correction :**

Réseau Destination	Interface	Routeur Suivant	Type	Commentaire
0.0.0.0/0	b1	10.0.0.14	DISTANT	C1 routeur par défaut
192.168.1.0/24	a1	0.0.0.0	DIRECT	Son réseau interne
192.168.2.0/24	b1	10.0.0.14	DISTANT	C1 routeur par défaut
192.168.3.0/24	b1	10.0.0.14	DISTANT	C1 routeur par défaut

Autre réponse possible :

Réseau Destination	Interface	Routeur Suivant	Type	Commentaire
0.0.0.0/0	b1	10.0.0.14	DISTANT	C1 routeur par défaut
192.168.1.0/24	a1	0.0.0.0	DIRECT	Son réseau interne

Autre réponse possible :

Réseau Destination	Interface	Routeur Suivant	Type	Commentaire
0.0.0.0/0	b1	10.0.0.14	DISTANT	C1 routeur par défaut
192.168.1.0/24	a1	0.0.0.0	DIRECT	Son réseau interne
192.168.2.0/24	c1	10.0.0.21	DISTANT	C2 meilleur chemin
192.168.3.0/24	b1	10.0.0.14	DISTANT	C1 routeur par défaut

Autre possibilité :

Réseau Destination	Interface	Routeur Suivant	Type	Commentaire
0.0.0.0/0	b1	10.0.0.14	DISTANT	C1 routeur par défaut
192.168.1.0/24	a1	0.0.0.0	DIRECT	Son réseau interne
192.168.2.0/24	c1	10.0.0.21	DISTANT	C2 meilleur chemin

**Question 2 (3,5 points) :** Tous les liens des feuilles vers les routeurs de cœur ont un débit de 1Gb/s (coût 4) et les liens entre routeurs de cœur ont un débit de 10Gb/s (coût 2). Les liens ont le même débit dans les 2 sens donc le même coût.

- Si on exécute OSPF **uniquement dans le réseau** cœur quelle est la base de données qui contient l'état des liens correspondant au réseau 10.0.0.0/24 et qu'on va trouver répliquée dans chacun de ses routeurs. Chaque lien ne sera représenté qu'une fois dans la base pour simplifier la réponse. Compléter la base ci-dessous. **(1 point)**

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

**Correction :**

Lien	Coût du lien	N°séquence	Age
R1-C1	4	0	3600
R1-C2	4	0	3600
R2-C2	4	0	3600
R2-C3	4	0	3600
R3-C3	4	0	3600
R3-C1	4	0	3600
C1-C2	2	0	3600
C2-C3	2	0	3600
C3-C1	2	0	3600

- Quelle est la table de routage de C1 qui résulte du calcul du routage optimal par OSPF (donc par l'algorithme de Dijkstra). Si deux chemins ont un coût égal on les met tous les deux dans la table de routage, la politique du routeur est alors d'équilibrer la charge des liens. Ajouter des lignes à la table si cela vous est nécessaire. **(1 point)**

Attention, **OSPF**, sans indication particulière, n'utilise **pas de route par défaut**.

**Correction :**

Destination	Interface	Routeur Suivant	Type	Coût
C2	n1	10.0.0.72	DIRECT	2
C3	o1	10.0.0.62	DIRECT	2
R1	m1	10.0.0.11	DIRECT	4
R2	n1	10.0.0.72	DISTANT	6
R2	o1	10.0.0.62	DISTANT	6
R3	p1	10.0.0.31	DIRECT	4



- C2 tombe en panne, quelle est la nouvelle base de données d'état des liens, et quelle est la nouvelle table de routage de C1. Pour la base de données d'état des liens vous utiliserez le tableau ci-après, on a retiré la colonne Age pour simplifier. Si vous avez besoin de rajouter des liens dans la table de routage, ne pas hésiter à le faire. **(1,5 points)**

**Correction :**

Lien	Coût du lien	N°séquence
R1-C1	4	0
R1-C2	$+\infty$	1
R2-C2	$+\infty$	1
R2-C3	4	0
R3-C3	4	0
R3-C1	4	0
C1-C2	$+\infty$	1
C2-C3	$+\infty$	1
C3-C1	2	0

Toutes les routes vont devoir éviter C2. C'est ce que l'algorithme de calcul du meilleur chemin va donner (Dijkstra).

Destination	Interface	Routeur Suivant	Type	Coût
C2	n1	NONE	FAIL	$+\infty$
C3	o1	10.0.0.62	DIRECT	2
R1	m1	10.0.0.11	DIRECT	4
R2	o1	10.0.0.62	DISTANT	6
R3	p1	10.0.0.31	DIRECT	4

**Question 3 (3 points) :** On s'intéresse au multicast IP à travers le réseau précédent. On observe la trame suivante, une trame IGMP (Internet Group Management Protocol) dans le réseau 192.168.1.0/24 (celui accroché à R1).

```
9 77.106098      192.168.1.66      224.0.0.22      IGMP...      60 Membership Report / Join group 239.195.7.2 for any sources
> Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
✓ Ethernet II, Src: CiscoSpv_51:c3:81 (00:25:2e:51:c3:81), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
  ✓ Destination: IPv4mcast_16 (01:00:5e:00:00:16)
    Address: IPv4mcast_16 (01:00:5e:00:00:16)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..1. .... = IG bit: Group address (multicast/broadcast)
  ✓ Source: CiscoSpv_51:c3:81 (00:25:2e:51:c3:81)
    Address: CiscoSpv_51:c3:81 (00:25:2e:51:c3:81)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Padding: 000000000000
  ✓ Internet Protocol Version 4, Src: 192.168.1.66, Dst: 224.0.0.22
    0100 .... = Version: 4
    .... 0110 = Header Length: 24 bytes (6)
  > Differentiated Services Field: 0x58 (DSCP: AF23, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0060 (96)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (2)
    Header checksum: 0x8217 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.66
    Destination: 224.0.0.22
  > Options: (4 bytes), Router Alert
  ✓ Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Reserved: 00
    Checksum: 0xe338 [correct]
    [Checksum Status: Good]
    Reserved: 0000
    Num Group Records: 1
  > Group Record : 239.195.7.2  Change To Exclude Mode
```

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.

Numéro de copie :

- L'adresse MAC destination 01:00:5e:00:00:16 est une adresse de diffusion pourquoi ? **(0,5 point)**

**Correction :**

Le dernier bit à droite du premier octet de l'adresse MAC est à 1. Cela veut dire que l'adresse Ethernet est potentiellement une adresse vers un groupe de cartes NIC.

- L'adresse IP destination 224.0.0.22 est une adresse multicast IP. Le rôle d'IGMP est de gérer notamment des demandes d'adhésion à un groupe (Join) ou de retrait d'un groupe (Leave) ou de rapport (Report). 224.0.0.22 est utilisée pour l'envoi de rapport IGMPv3. Il est dit " 224.0.0.0 à 224.0.0.255 sont locales à un lien". Pourquoi, d'un point de vue fonctionnel, cette adresse ne peut être routée hors de 192.168.1.0/24 ? **(0,5 point)**  
Cela n'a rien à voir avec le fait que les adresses IP des réseaux, qui servent dans l'architecture étudiée, soient des adresses IP privées de type RFC1918.

**Correction :**

IGMP sert à rentrer et sortir d'un groupe IPMulticast. Formulé autrement, il sert à s'abonner et à se désabonner pour des membres d'un même réseau IP. Par conséquent, les datagrammes IGMP ne sont pas destinés à être propagés hors du réseau IP dans lequel ils sont générés.

Normalement le TTL d'un datagramme IGMP devrait être de 1, ce qu'on peut vérifier dans la trace Wireshark.

- L'encapsulation d'un paquet IP multicast dans une trame Ethernet multicast suit une procédure particulière pour la mise en correspondance adresse MAC-adresse IP multicast. Le processus est le suivant :
  - on prend les 23 derniers bits de l'adresse IP et ils deviennent les 23 derniers bits de l'adresse MAC
  - les 25 premiers bits de l'adresse MAC sont fixés à : 01-00-5E-00-00-00

On a bien 48 bits d'adresse MAC.

Exemple : 224.1.2.3 donne 01-00-5E-01-02-03.

Il peut y avoir des collisions : collision d'adresse MAC multicast : 225.129.2.3 donne aussi 01-00-5E-01-02-03

Vérifier que 224.0.0.22 donne bien 01:00:5e:00:00:16. **(1 point)**

**Correction :**

On va prendre les 23 derniers bits de 224.0.0.22, on obtient : 000 0000.0000 0000.0001 0110 soit 00-00-16

On rajoute le préfixe 01-00-5E-00-00-16 et on obtient bien l'adresse MAC attendue.

- Quelle va être l'adresse MAC Multicast qui va correspondre à 239.195.7.2, qui est l'adresse du groupe auquel 192.168.1.66 appartient ? **(1 point)**

**Correction :**

Pour 239.195.7.2, c'est le même raisonnement. On prend les 23 derniers bits de l'adresse IP, ce qui donne 100 0011.0000 0111.0000 0010 soit 43-07-02. On obtient l'adresse MAC 01-00-5E-43-07-02.

**Question 4 (2 points) :** Tous les routeurs de l'architecture savent router des datagrammes IP multicast, et si C1 est la racine d'un arbre de diffusion IP multicast partagé, qu'on appelle aussi "Rendez-vous Point". R1, R2, R3, C1, C2, C3 connaissent tous l'adresse IP 239.195.7.2.

On suppose qu'une interface dans 192.168.2.0/24 est abonnée à 239.195.7.2.

On suppose qu'une interface dans 192.168.3.0/24 est abonnée à 239.195.7.2.

On suppose qu'une interface dans 192.168.1.0/24, différente de 192.168.1.66, est abonnée à 239.195.7.2.

L'interface 192.168.1.66 souhaite diffuser un datagramme IP sur 239.195.7.2.

- Proposez une trajectoire qui n'utilise que de l'Unicast en passant par C1. **(0,5 point)**

**Correction :**

Il faut faire l'hypothèse que 192.168.1.66 connaît tous les destinataires du message, donc connaît toutes les adresses IP correspondantes de ses destinataires. A partir de là, 192.168.1.66 envoie autant de datagrammes en unicast qu'il y a de destinataires.

La question essentielle ici c'est, comment 192.168.1.66 connaît les membres du groupe multicast. On peut stocker cette liste dans un annuaire distribué voire répliqué par exemple. Les routeurs qui exécutent IGMP pourraient être éligibles à héberger une partie de cet annuaire. Se pose alors la question de la gestion de l'appartenance à un groupe IP multicast, et du moment à partir duquel un membre est ou n'est pas dans la liste des membres du groupe car bien sûr les membres entrent et sortent du groupe de façon asynchrone tant pour la gestion du groupe que pour l'envoi et la réception des datagrammes multicast.

C'est peu efficace, mais ça fonctionne.

- Proposez une trajectoire qui utilise un principe de diffusion de routeur en routeur en passant par C1. **(1 point)**

**Correction :**

Cette fois, 192.168.1.66 doit envoyer un datagramme en unicast à C1 qui est la racine de l'arbre de diffusion IP multicast. On dit aussi que C1 est un point de rendez-vous<sup>2</sup> (RP, RdV point dans la terminologie PIM-SM, Protocol Independant Multicast – Sparce Mode). Une fois reçu, le datagramme va être émis par C1 avec une l'adresse IP multicast de destination 239.195.7.2. Les routeurs appartenant à l'arbre de diffusion vont relayer le datagramme de routeur en routeur. C'est comme ça que le datagramme va parcourir une vague qui va atteindre C2 ou C3 pour atteindre R2 ainsi que R1 et R3. Une fois sur les Ri (i=1 à 3), le datagramme pourra être propagé vers les abonnés avec toujours l'adresse 239.195.7.2.

Une question se pose : comment l'arbre de diffusion est-il construit ? L'arbre se construit par greffe quand un routeur a des abonnés pour un groupe, il se connecte au prochain routeur vers la racine pour recevoir le flux multicast. Au contraire, quand il ne doit plus propager de trafic multicast, car il n'a plus d'abonné, il effectue un élagage de sa branche par rapport à l'arbre de routage multicast.

Une question reste en suspend : quelle est l'adresse source du datagramme pour joindre C1 ?

- Cela peut être 239.195.7.2 dans le champ IPdest du datagramme, ce qui nécessite que R1, qui est le routeur d'abonnement via IGMP de 192.168.1.66, sache que pour l'adresse IP destination 293.195.7.2 il faut envoyer les datagrammes à C1. Mais dans ce cas, comment R1 distingue un datagramme de diffusion vers C1, d'un datagramme de diffusion vers les abonnés de l'adresse IP multicast.
  - Cela peut être l'adresse IP de C1 dans IPdest du datagramme. Là c'est simple.
  - La solution dans PIM-SM est une combinaison des deux. L'émetteur 192.168.1.66 envoie son datagramme avec l'adresse IPdes 239.195.7.2. Son routeur associé pour le protocole IPmulticast encapsule ce datagramme dans un datagramme envoyé en unicast avec IPdest = C1.
- Quelle recommandation feriez vous pour construire un arbre de diffusion partagé tel que le routage sur cet arbre soit le plus optimal possible sachant que vous avez déjà bâti une architecture à routage OSPF sur le réseau qu'emprunte le Multicast IP. **(0,5 point)**

**Correction :**

Le souci avec ce qu'on vient de voir, c'est qu'il faut toujours aller à un point de rendez-vous. Si l'émetteur envoie souvent des messages, passer par le RP ralentit la transmission. Idéalement il faudrait que l'émetteur le plus fréquent devienne le RP. C'est une des fonctionnalités comprises dans PIM-SM.

---

<sup>2</sup> Cette terminologie n'a pas été vue en cours, ce n'est donc pas une réponse attendue. Mais le corrigé est une bonne opportunité pour présenter qq concepts de plus au cours.

➔ Vérifiez que vous disposez bien de la totalité des pages du sujet en début d'épreuve et signalez tout problème de reprographie le cas échéant.