

Exo_1: TCP

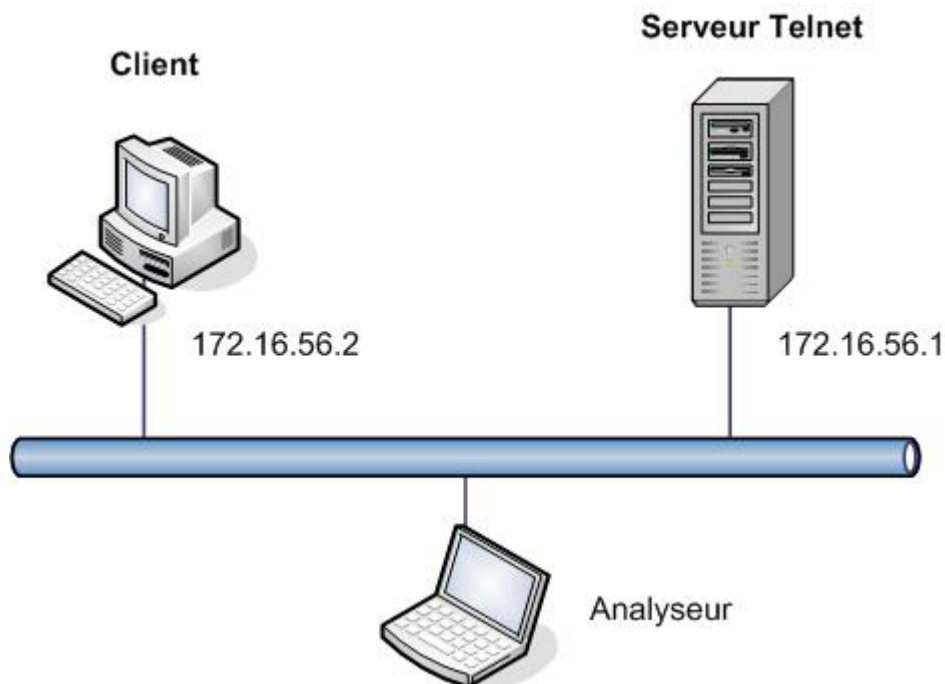
Objectifs du TP → identifier les différentes phases d'un échange TCP: connexion, échange de données et déconnexion ainsi que les principaux champs de l'entête TCP.

Pour vous aider, téléchargez auparavant le document suivant:

- TCP_RFC793.pdf

1) Lancer votre analyseur "Ethereal" et chargez la trace jointe avec cet exo intitulée "TP_echange TCP.cap".

Celle-ci a été relevée dans l'environnement suivant: une station cliente telnet se connecte sur un serveur telnet, puis crée un répertoire sur celui-ci et ensuite se déconnecte.



Dans le menu d'Ethereal, allez dans *Edit* → *Préférences.....* à gauche dans *protocole* sélectionnez *TCP* et décochez *Relative sequence numbers and window scaling*

Analyze TCP sequence numbers:	<input checked="" type="checkbox"/>
Relative sequence numbers and window scaling:	<input type="checkbox"/>
Try heuristic sub-dissectors first:	<input type="checkbox"/>

2) Pointez sur la **trame N° 3**, et développez (détaillez) le protocole TCP ainsi que son champ flags, en validant le + en début de ligne !

The screenshot shows the Wireshark interface with a packet capture of a Telnet connection. The packet list at the top shows frame 3 as a TCP SYN packet. The packet details pane is expanded to show the TCP header and flags. Two callout boxes point to the TCP section and the flags field.

Packet List:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.56.2	Broadcast	ARP	who has 172.16.56.1? Tell 172.16.56.2
2	0.000210	172.16.56.1	172.16.56.2	ARP	172.16.56.1 is at 00:08:74:9f:a0:37
3	0.000428	172.16.56.2	172.16.56.1	TCP	1054 > telnet [SYN] Seq=2480510162 Ack=0 win=16384
4	0.000752	172.16.56.1	172.16.56.2	TCP	telnet > 1054 [SYN, ACK] Seq=449923941 Ack=2480510162
5	0.000755	172.16.56.2	172.16.56.1	TCP	1054 > telnet [ACK] Seq=2480510163 Ack=449923942 win=16384
6	0.002551	172.16.56.1	172.16.56.2	TELNET	Telnet Data ...
7	0.002770	172.16.56.1	172.16.56.2	TELNET	Telnet Data ...

Packet Details (Frame 3):

- Frame 3 (62 bytes on wire (49 bytes captured) on interface 0)
- Ethernet II, Src: 172.16.56.2 (00:02:3f:b4:c3:49), Dst: 172.16.56.1 (00:08:74:9f:a0:37)
- Internet Protocol, Src: 172.16.56.2 (172.16.56.2), Dst: 172.16.56.1 (172.16.56.1)
- Transmission Control Protocol, Src Port: 1054 (1054), Dst Port: telnet (23), Seq: 2480510162, Ack: 0, Len: 0
 - Source port: 1054 (1054)
 - Destination port: telnet (23)
 - Sequence number: 2480510162
 - Header length: 28 bytes
 - Flags: 0x0002 (SYN)
 - 0... .. = Congestion Window Reduced (CWR): Not set
 - .0.. .. = ECN-Echo: Not set
 - ..0. .. = Urgent: Not set
 - ...0 .. = Acknowledgment: Not set
 - 0.. = Push: Not set
 -0. = Reset: Not set
 -1. = Syn: Set
 -0 = Fin: Not set
 - window size: 16384
 - checksum: 0x4e1a [correct]
 - Options: (8 bytes)

Packet Bytes:

```

0000  00 08 74 9f a0 37 00 02 3f b4 c3 49 08 00 45 00  ..t..7..?..I..E.
0010  00 30 03 ae 40 00 80 06 2e f6 ac 10 38 02 ac 10  .0..@...8...
0020  38 01 04 1e 00 17 93 d9 94 d2 00 00 00 00 70 02  8.....p
0030  40 00 4e 1a 00 00 02 04 05 b4 01 01 04 02      @.N.....
  
```

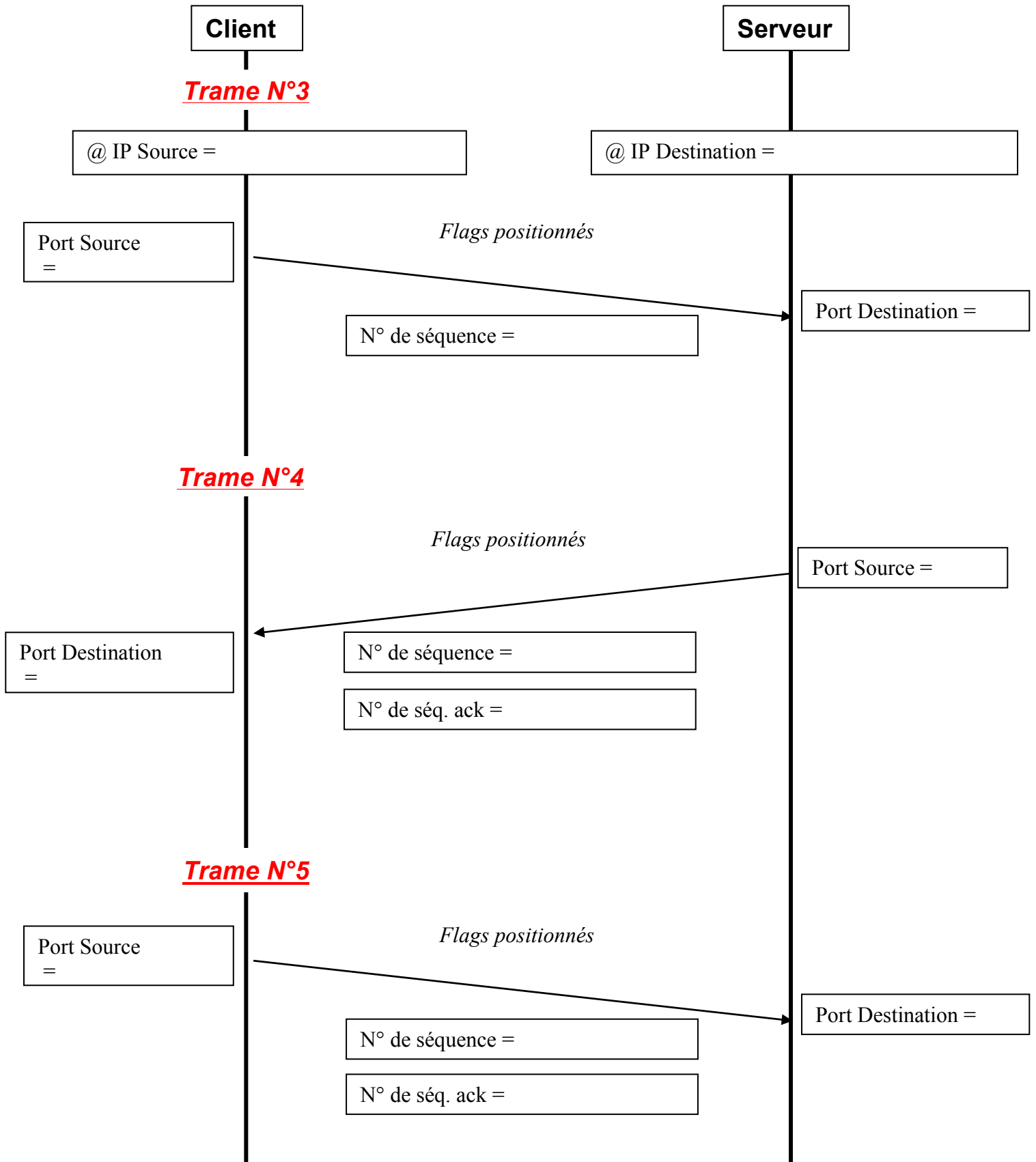
Callout boxes:

- Développez TCP (points to the Transmission Control Protocol section)
- Développez les flags (points to the Flags field)

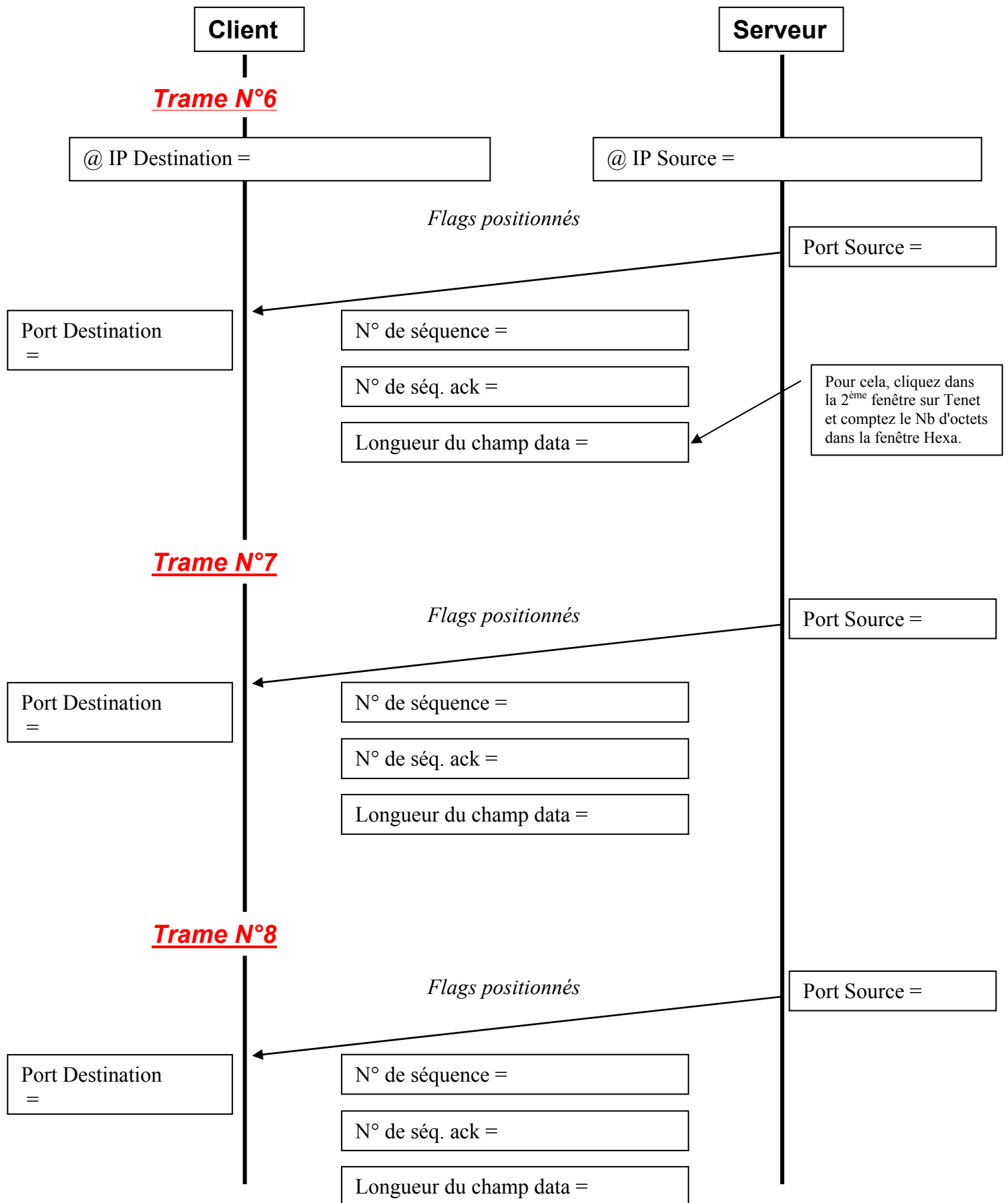
puis au regard des trames échangées répondez aux questions suivantes en remplissant les cases des différentes trames demandées:

- @ IP source et @ IP destination
- Port source et port destination
- Les flags positionnés (Syn, Ack, Push, Fin, etc...)
- Les numéros de séquences
- Les numéros de séquences acquittés
- Longueur du champ data (éventuellement)

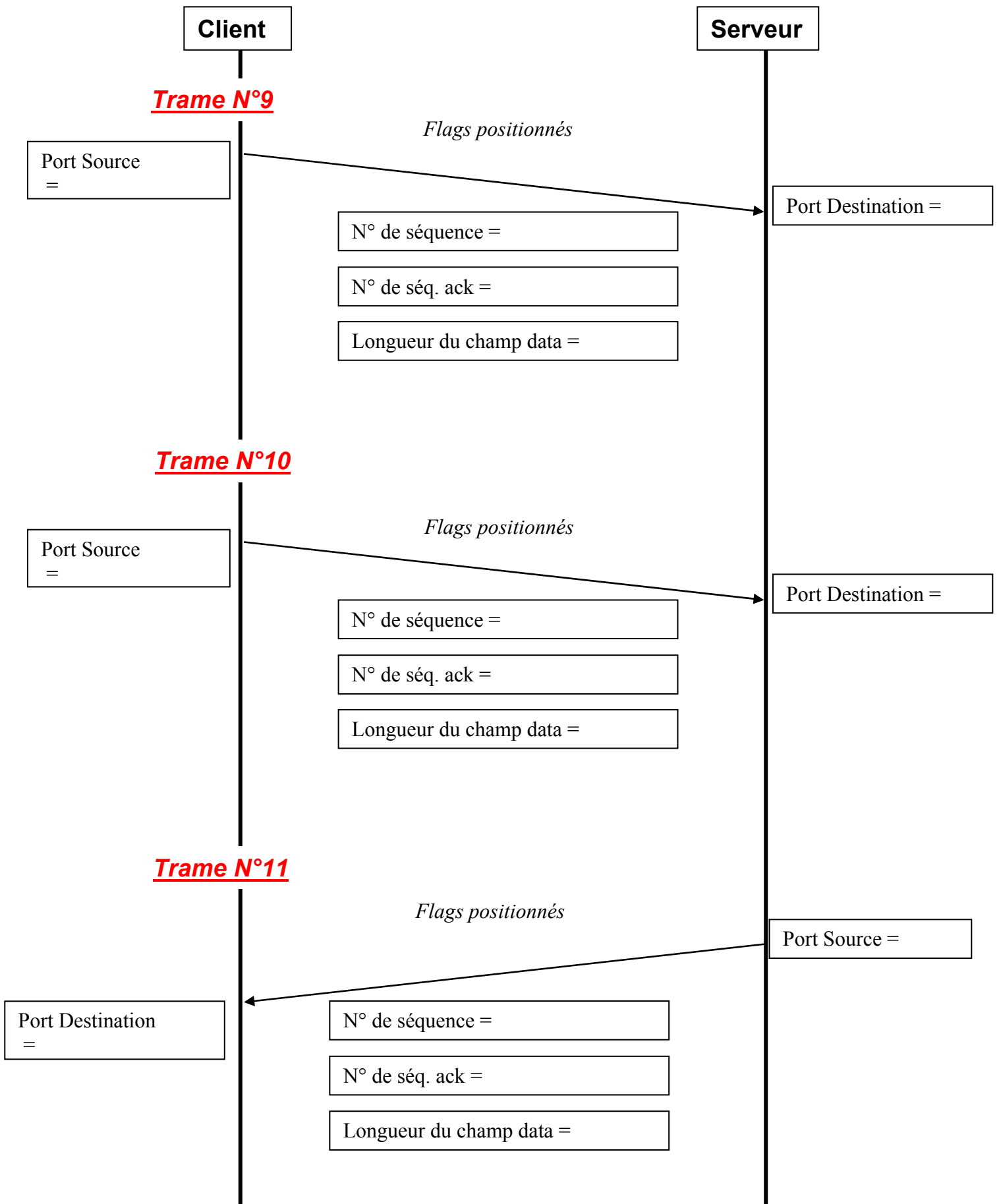
Phase de connexion

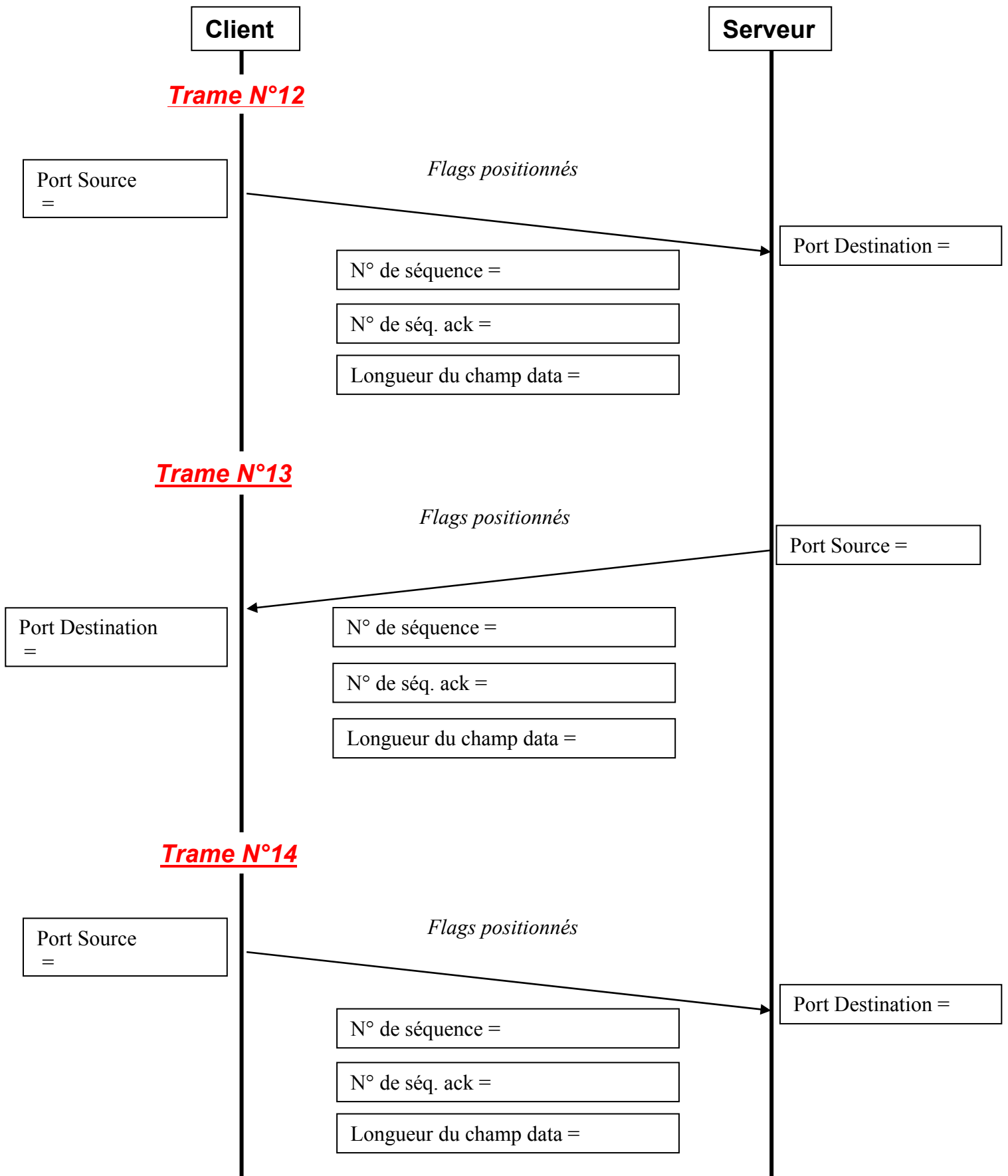


Phase d'échange

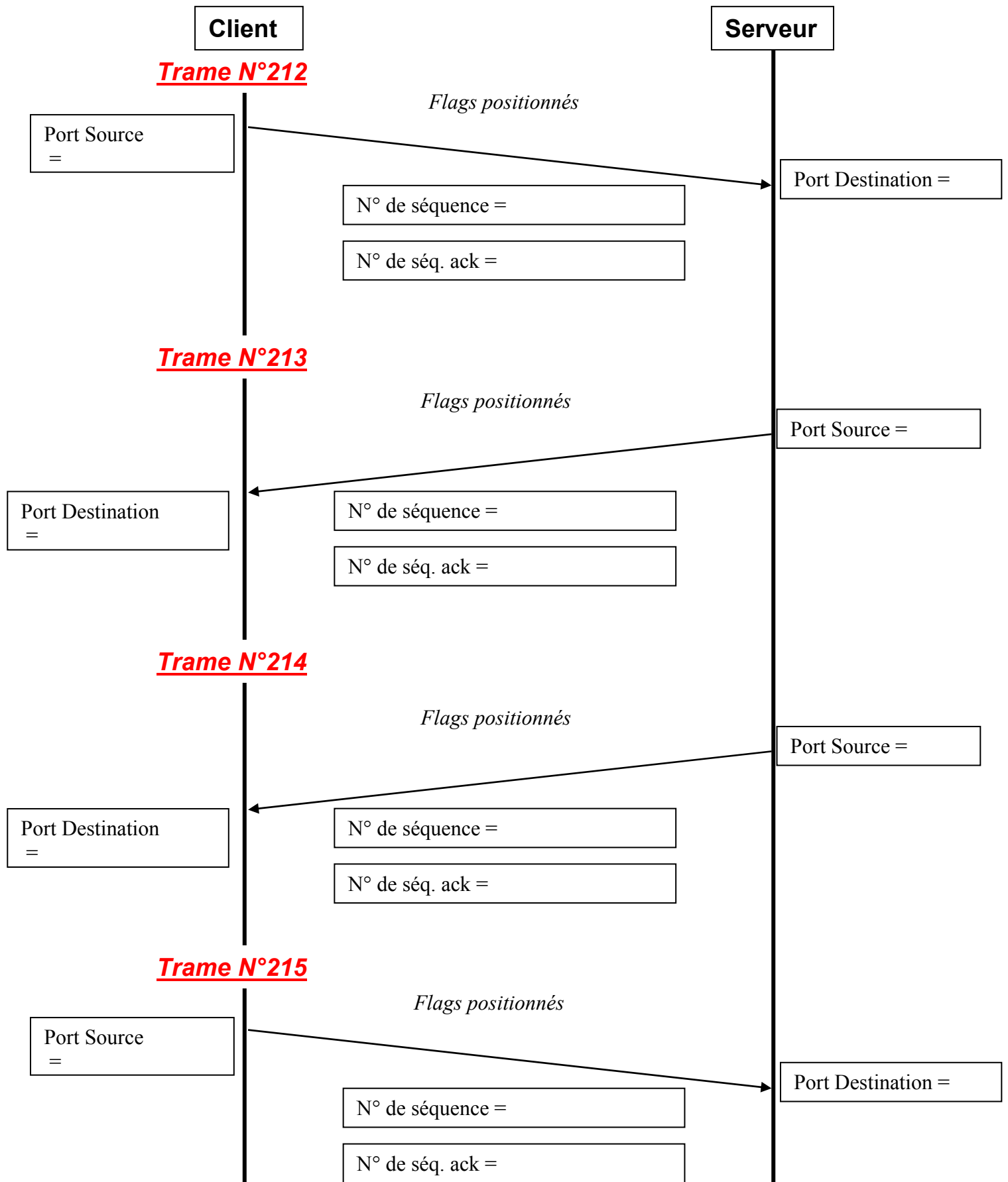


EXERCICE TCP





Phase de déconnexion



Correction

Dans le menu d'Ethereal, allez dans *Statistics* → *Flow Graph* et sélectionnez *General flow* puis valider par *OK*.

