UFR IM²AG

UNIVERSITÉ Grenoble Alpes

Examen Administration de réseaux
Master Informatique 1ère année 2022

P. Sicard

mardi 3 mai 2022

Durée : 3 heures
Tous documents autorisés. Calculatrices autorisées. Ordinateurs interdits.
Un barème approximatif est donné.

1 ADMINISTRATION D'UN INTRANET (11 points)

Vous devez administrer l'Intranet présenté sur la figure 2 de l'annexe 1.
Il est composé de trois switchs Ethernet, des machines hôtes (*A, B, C, D* et deux routeurs *R1* et *R2*. Le routeur *R1* possède une interface ADSL (ligne téléphonique) et une interface Ethernet (reliée au switch 1). La figure 2 de l'annexe 1 donne aussi les numéros de port utilisés sur les switchs (réels) 1, 2 et 3.

Le fournisseur d'accès à Internet vous propose d'utiliser une seule adresse publique. Le routeur *R1* doit être configuré pour son interface ADSL (sortie vers Internet) avec l'adresse **100.0.0.66/30**. Le premier routeur d'Internet (noté *Rext* sur le plan) possède l'adresse **100.0.0.65/30**.

1.1 RESEAU VIRTUEL (VLAN VIRTUAL LOCAL AREA NETWORK) (3 points)

A partir de ce réseau réel, nous voulons créer des réseaux virtuels pour aboutir à l'Intranet virtuel donné dans la figure 3 (voir Annexe 2). Quatre VLANs doivent être créés :

— VLAN 1 : le routeur *R1*, l'hôte *D* et le routeur *R2*,
— VLAN 2 : l'hôte *A* et le routeur *R2*,
— VLAN 3 : l'hôte *B* et le routeur *R2*,
— VLAN 4 : l'hôte *C* et le routeur *R2*.

— Le routeur *R2* possèdent donc 4 interfaces (virtuelles).

1. Quels sont les ports des switchs sur lesquels les trames doivent obligatoirement être étiquetées ? Pourquoi ?

2. Sur quels ordinateurs et quelles interfaces les trames doivent-elles obligatoirement être étiquetées ? Pourquoi ?

3. Donnez les associations Ports/VLAN des trois switchs (réels) permettant la mise en place de ces réseaux virtuels.

4. Donnez les paquets que l'on devrait capturer sur le routeur *R2* lors d'un ping de l'hôte A vers l'hôte D. Pour chacun des paquets, précisez le numero de *vlan* porté par le paquet et l'interface de *R2* sur laquelle est capturé le paquet. On suppose les tables ARP vides sur toutes les machines avant le *ping*.

1.2 PLAN D'ADRESSAGE PRIVE ET TRANSLATION D'ADRESSE (4 points)

A partir de là vous devez travailler sur le plan donné dans la figure 3 de l'annexe 2. Vous pouvez donc répondre aux questions même si vous n'avez pas fait la partie précédente sur les *VLANs*.

On suppose que la seule adresse publique que vous avez à votre disposition est celle du routeur *R1* (**100.0.0.66/30**).

1. Proposez un plan d'adressage du réseau virtuel obtenu à partir d'adresses IPv4 privées.

Remarque : Vous pouvez rendre le plan de la figure 3 (annexe 2) annotée des adresses des routeurs et des ordinateurs hôtes.

2. Donnez les tables de routage des hôtes *A* et *D* et des deux routeurs *R1* et *R2* de telle manière que :
   — Tous les hôtes doivent pouvoir accéder à Internet.
   — Tous les hôtes doivent pouvoir communiquer entre eux.
   — Les tables de routages possédent le moins possible de ligne.
   On donnera les tables de routage sous la forme :
   Réseau destination | *Netmask (ou notation /x)* | *Adresse du routeur voisin*

   Remarques :
   — Pour simplifier la lecture de ces tables, il est fortement conseillé d'utiliser des noms au lieu des adresses (à préciser dans le plan d'adressage).
   — Attention les routeurs possèdent plusieurs adresses.
   — Rappelez les lignes de connexions directes aux réseaux qui apparaissent à l'initialisation des interfaces dans ces tables de routage.

3. Expliquez comment configurer une translation d'adresse sur le routeur *R1* avec le plan d'adressage donné dans la question précédente. On donnera le type de translation d'adresse (statique/dynamique) et la (ou les) plages d'adresses publiques et privées utilisées.

4. Donnez le contenu de la table NAT dans le routeur *R1* pendant qu'une connexion TCP est ouverte vers un serveur WEB existant sur une machine extérieure d'adresse *192.0.0.1* depuis l'hôte *A*.
   On donnera la table NAT sous la forme : *Adresse publique* | *Adresse privée* | *Numéro de Port* | *Numéro de Port Translaté*

5. On veut mettre en place un serveur *ssh* sur l'hôte *A* accessible depuis l'extérieur. Expliquez comment procéder et donnez la partie de la table NAT nécessaire.

1.3 FILTRAGE (2,5 points)

On veut mettre en place des restrictions d'accès à l'Intranet.

Le format des règles d'accès est :
Adr. source/ Adr. destination/ Port source/ Port destination/ Protocole /flags /Autorisé-Interdit

On précisera sur quelle interface du (ou des) routeurs les règles sont mises en place et pour quels paquets entrant ou sortant dans l'interface (depuis ou vers le réseau) les règles sont appliquées (comme sur les routeurs Cisco que vous avez configurés en travaux pratiques).
Remarques : faire attention au fait que les filtres peuvent suivant vos choix, être avant la translation d'adresse (intérieur de l'Intranet) ou après la translation d'adresse (sortie/entrée extérieur du routeur R1).

1. Donnez les règles du pare-feu à mettre en place sur le routeur *R2* permettant de :
   — Laisser entrer (vers *A, B* et *C*) les paquets provenant de l'hôte *D*.
   — Réciproquement laisser sortir les paquets vers l'hôte *D*.
   — Laisser entrer dans l'Intranet les flux vers le serveur *ssh* se trouvant sur la machine *A*.
   — Laisser sortir de l'Intranet les flux depuis le serveur *ssh* se trouvant sur la machine *A*.
   — Tous les autres paquets doivent être détruits.

2. Donnez les règles du pare-feu à mettre en place sur le routeur *R1* permettant de :
   — Laisser entrer dans l'Intranet les flux vers le serveur *ssh* se trouvant sur la machine *A*.
   — Laisser sortir de l'Intranet les flux depuis le serveur *ssh* se trouvant sur la machine *A*.
   — Laisser entrer dans l'Intranet tous les paquets à destination de *D*.
   — Laisser sortir de l'Intranet tous les paquets issus de *D*.
   — Tous les autres paquets doivent être détruits.

3. Avec ces règles, on veut que les utilisateurs des machines A,B et C puissent naviguer sur le WEB.
   Expliquez comment procéder (utilisation de proxys, configuration particulière de navigateur WEB...).
4. Avec ces règles un utilisateur se situant sur une machine extérieure à l'Intranet peut-il transférer des fichiers sur l'hôte A. Si oui comment peux t-il procéder ?

1.4 QUALITE DE SERVICE (1,5 points)

On veut privilégier les communications de l'hôte A avec l'extérieur (par rapport à celles de B et C).

Expliquez en 10 lignes comment procéder en précisant :

— Sur quel(s) routeur(s) ou machine(s) agir ?
— Quels mécanismes mettre en place ?
— Peux t-on mettre en place cette priorité au niveau d'une application particulière ? Si oui comment ?

2 PROTOCOLE TCP (5 points)

En annexe 3 sont données les traces de captures de paquets sur un ordinateur relié à un réseau Ethernet à l'aide de l'outil Wireshark.
La première colonne donne le numéro du paquet, la deuxième le temps écoulé depuis le début de la capture (en seconde).
Ensuite pour chaque paquet sont donnés :

- les adresses IP source et destination,
- le protocole de niveau le plus haut,
- les valeurs de certains champs de l'entête TCP : les numéros de port source et destination,
- des flags éventuels, le numéro de séquence (**Seq**),
- le numéro d'acquittement (**Ack**),
- la valeur de la fenêtre du récepteur (**Win**),
- la taille des données TCP **(Len)**.

Cette capture a été effectuée après l'ouverture d'une connexion TCP entre deux machines lors de l'envoi de données (en grande quantité) à travers cette connexion. La capture a été effectuée sur la machine d'adresse *193.0.0.1*.

L'annexe 4 contient la courbe d'évolution des numéros de séquence TCP (en foncé), des numéros d'acquittement TCP (en clair) et du dernier numéro de séquence pouvant être réceptionné (champ WIN de TCP + numéro d'acquittement). Le temps sur les abscisses est donné en seconde. Pour certains paquets il est donné le numéro du paquet apparaissant dans l'annexe 3.
Remarque : on pourra rendre la courbe commentée de l'annexe 4 avec sa copie.

Répondre aux questions suivantes :

1. Le paquet 496 semble être un acquittement TCP (sans donnée). Jusqu'à quel paquet de donnée est-il l'acquittement ? Comment le savez vous ?
2. La taille du buffer d'émission est de 32 000 et celle du buffer de réception est de 66 608 octets sur les deux machines. La figure 1 ci dessous montre les deux fenêtres de contrôle de flux (gris foncé) et de récupération d'erreur (gris clair) sur la machine 193.0.0.1 après la réception du paquet 496.
   Donnez les valeurs de :
   - No Seq Dernier Octet Lu : numéro de séquence du dernier octet lu par l'application sur la machine 192.0.0.1
   - No Seq Dernier octet Emis : Numéro de séquence du dernier octet émis par la machine 193.0.0.1
   - No Seq FCE : numéro du dernier octet pouvant être émis à cause de la fenêtre du contrôle d'erreur (en fait sa limite)
   - No Seq FCF : numéro du dernier octet pouvant être émis à cause de la fenêtre du contrôle de flux (en fait sa limite)
3. La taille de la fenêtre de contrôle de congestion au début de la capture est de 14*MSS octets

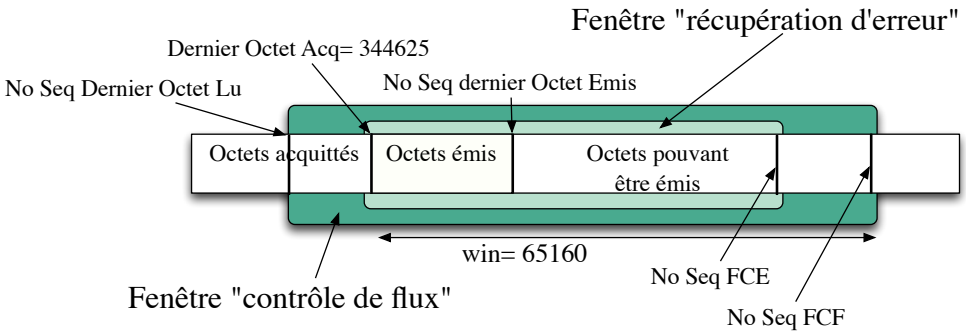

Figure 1 – Fenêtres à anticipation

(MSS est la taille maximale des paquets sur le réseau, soit ici 1448 octets de données TCP). Où retrouve t-on cette taille de la fenêtre de congestion sur la courbe de l'annexe 4.

4. Complétez la figure 1 en faisant apparaître la fenêtre de contrôle de congestion. Précisez sa limite supérieure (numéro maximal de l'octet pouvant être envoyé).
5. L'émission des données est interrompue pendant 18 millisecondes entre le paquet 473 et 476. Pourquoi ? Quel est l'évènement qui a déclenché l'envoi du paquet 476 ? Pourquoi 12 paquets de données sont émis à la suite du paquet 476 ? (jusqu'au 497).
6. Le paquet 505 est noté TCP Retransmission par Wireshark. Pourquoi ? Quel est le paquet qui contient les mêmes octets de données que le paquet 505 ?
7. Pourquoi ce paquet est-il émis ? Quel est l'évènement qui a déclenché son émission ?
8. Quelle est la valeur de la fenêtre de contrôle de congestion et du seuil d'évitement de congestion après l'émission du paquet 505 ? Comment a t-il été calculé ? Comment peut-on le vérifier sur la courbe de l'annexe 4 ?
9. Qu'est ce qui permet l'envoi des paquets de donnée 516 à 527 ?
10. Quelle est la version du contrôle de congestion utilisé ici : Reno ou Tahoe ? Comment le savez vous ?
11. Expliquez en 3 lignes quelle est l'amélioration apportée par la version Reno par rapport à Tahoe ?

3 APPLICATION DNS (4 Points)

Voici les traces d'une capture de 10 paquets sur un réseau :

```
No      Source          Destination           Info
1   193.54.236.137    193.54.236.171    Standard  query  A  www.google.com
2   193.54.236.171    192.12.94.30      Standard  query  A  www.google.com
```

```
3   192.12.94.30      193.54.236.171   Standard  query  response
4   193.54.236.171    216.239.32.10    Standard  query  A  www.google.com
5   216.239.32.10     193.54.236.171   Standard  query  response  CNAME  www.l.google.com
6   193.54.236.171    216.239.38.10    Standard  query  A  www.l.google.com
7   216.239.38.10     193.54.236.171   Standard  query  response
8   193.54.236.171    209.85.137.9   Standard  query  A  www.l.google.com
9   209.85.137.9      193.54.236.171  Standard  query  response A 209.85.227.99 A 209.85.227.147
     A  209.85.227.103  A  209.85.227.104
10   193.54.236.171  193.54.236.137 Standard query response CNAME www.l.google.com
     A  209.85.227.99  A  209.85.227.103  A  209.85.227.104  A  209.85.227.147
```

Ces paquets ont été capturés à la suite d'un ***ping www.google.com*** sur la machine d'adresse ***193.54.236.137***. La machine d'adresse ***193.54.236.171*** est un serveur DNS.

Pour vous aider à répondre aux questions, voici les résultats de plusieurs appels de la commande *host* (sous Unix) permettant d'effectuer des interrogations DNS.
Rappel : l'option ***–t ns*** permet d'obtenir la liste des serveurs DNS d'un domaine.

```
$ host -t ns com.
com name server d.gtld-servers.net.
com name server f.gtld-servers.net.
com name server i.gtld-servers.net.
com name server b.gtld-servers.net.
com name server g.gtld-servers.net.
com name server m.gtld-servers.net.
com name server a.gtld-servers.net.
com name server e.gtld-servers.net.
com name server k.gtld-servers.net.
com name server h.gtld-servers.net.
com name server j.gtld-servers.net.
com name server c.gtld-servers.net.
com name server l.gtld-servers.net.

$ host 192.12.94.30
30.94.12.192.in-addr.arpa domain name pointer e.gtld-servers.net.

$ host -t ns google.com.
google.com name server ns3.google.com.
google.com name server ns2.google.com.
google.com name server ns1.google.com.
google.com name server ns4.google.com.

$ host 216.239.32.10
10.32.239.216.in-addr.arpa domain name pointer ns1.google.com.
```

```
$ host 216.239.38.10
10.38.239.216.in-addr.arpa domain name pointer ns4.google.com.

$ host -t ns l.google.com
l.google.com name server ns1.google.com.
l.google.com name server ns4.google.com.
l.google.com name server ns3.google.com.
l.google.com name server ns2.google.com.
```

Répondre aux questions suivantes :

1. A quoi sert le paquet 1 ? Que veut dire « Standard Query A » ?

2. A quoi sert le paquet 2 ? Quelle fonctionnalité (dans l'application DNS) possède la machine d'adresse 192.12.94.30 ?

3. Que contient la réponse contenue dans le paquet 3 ?

4. Pourquoi le serveur DNS d'adresse 193.54.236.171 n'a-t-il pas commencé par interroger un serveur de la zone racine (« . ») pour effectuer la résolution de nom DNS ?

5. A quoi sert le paquet 4 ? Quelle fonctionnalité (DNS) possède la machine d'adresse 216.239.32.10 ?

6. Que contient la réponse contenue dans le paquet 5 ? Que veut dire CNAME ?

7. A quoi sert le paquet 6 ? Pourquoi est-il adressé à la machine d'adresse 216.239.38.10 ? Quelle fonctionnalité (DNS) possède la machine d'adresse 216.239.38.10 ?

8. Que contient la réponse contenue dans le paquet 7 ? Pourquoi ce n'est pas une réponse de type A ?

9. Que contient le paquet 8 ? Pourquoi est-ce à nouveau une requête sur le nom www.l.google.com ?

10. Que contiennent les paquets 9 et 10 ? Pourquoi les mêmes adresses apparaissent elles dans ces deux derniers paquets ?

11. Vers quelle adresse IP le ping effectué au départ va t-il être envoyé ?

4 Annexes

Annexe 1

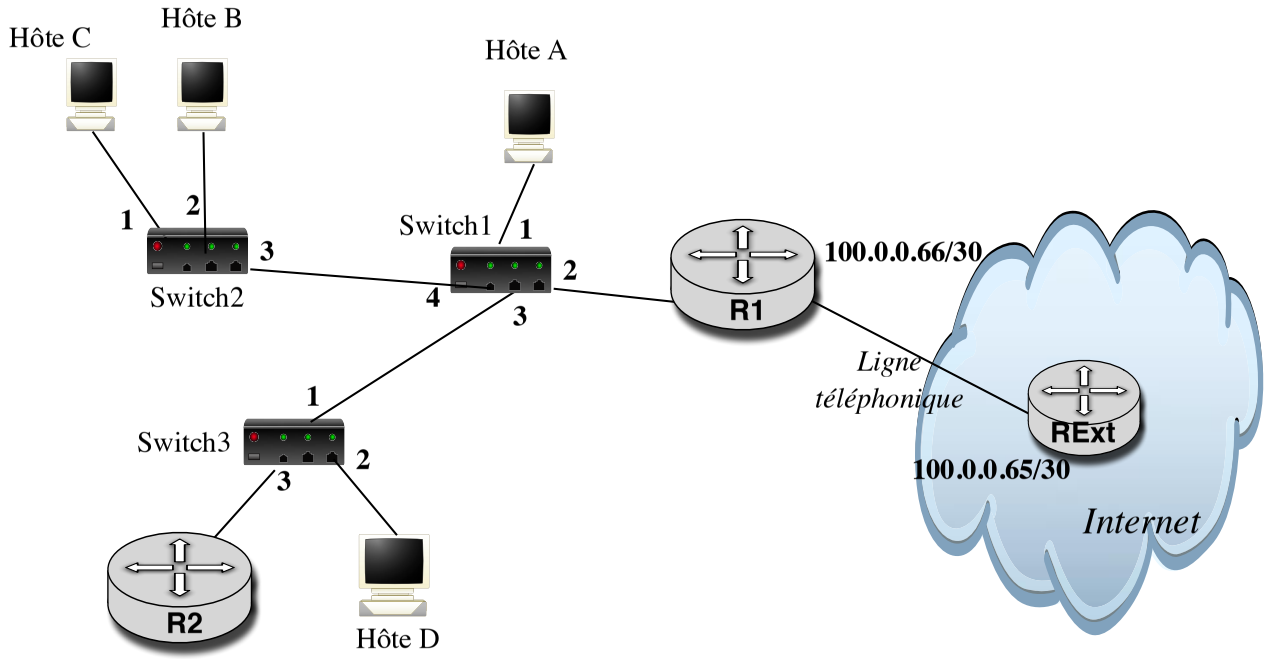

Figure 2 – Topologie du réseau à administrer

Annexe 2

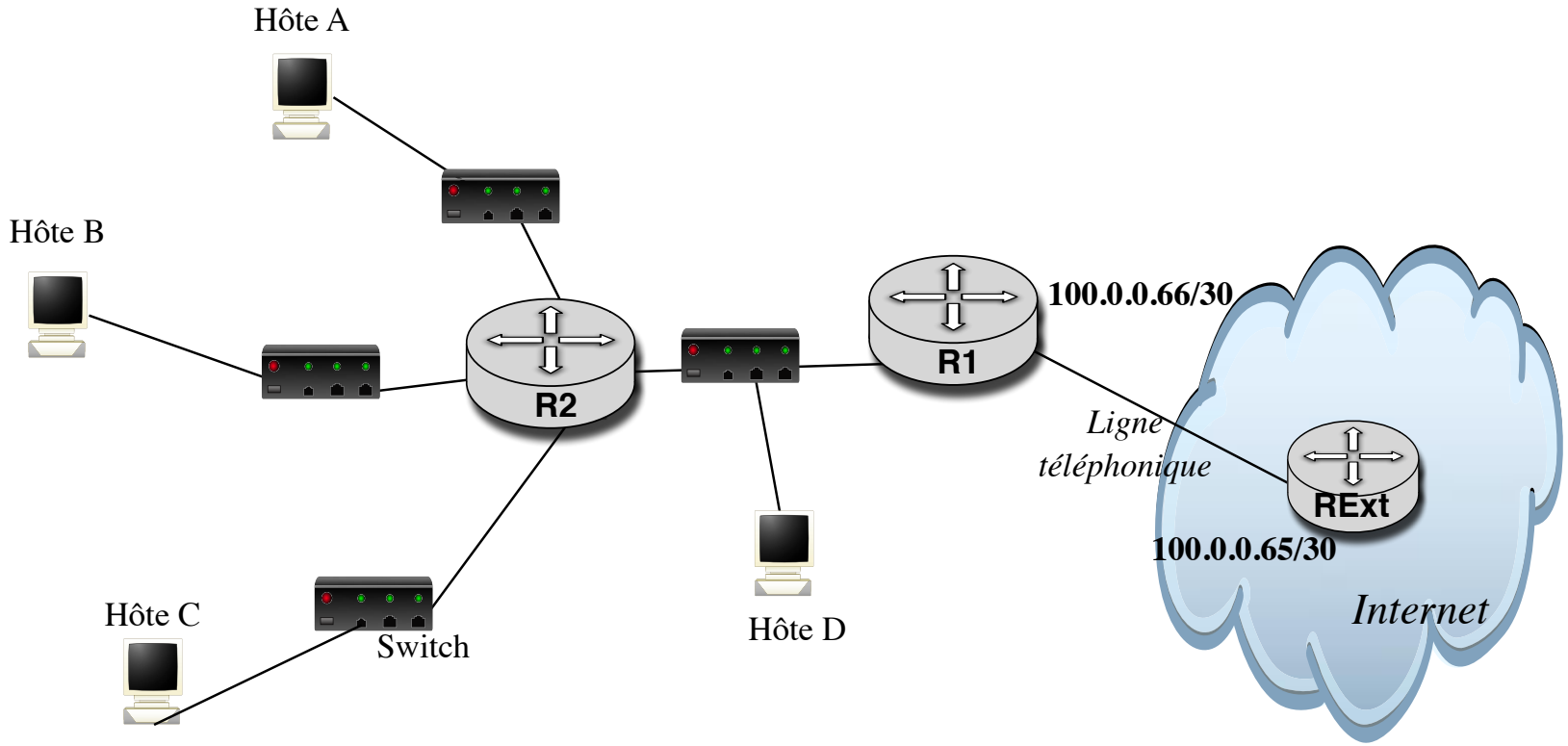

Figure 3 – Topologie du réseau virtuel

Annexe 3 : Résumés des paquets capturés

No.	*Time*	*Source*	*Destination*	*Protocole*	*Informations entête TCP*
469	0.558832	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=343177 Ack=1 Win=66608 Len=1448
470	0.558957	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=325801 Win=65160 Len=0
471	0.558983	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=344625 Ack=1 Win=66608 Len=1448
472	0.559055	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=327249 Win=65160 Len=0
473	0.559075	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=346073 Ack=1 Win=66608 Len=1448
474	0.577666	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=328697 Win=65160 Len=0
475	0.577669	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=330145 Win=65160 Len=0
476	0.577693	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=347521 Ack=1 Win=66608 Len=1448
477	0.577708	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=348969 Ack=1 Win=66608 Len=1448
478	0.577917	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=331593 Win=65160 Len=0
479	0.577919	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=333041 Win=65160 Len=0
480	0.577938	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=350417 Ack=1 Win=66608 Len=1448
481	0.577951	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=351865 Ack=1 Win=66608 Len=1448
482	0.578042	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=334489 Win=65160 Len=0
483	0.578061	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=353313 Ack=1 Win=66608 Len=1448
484	0.578166	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=335937 Win=65160 Len=0
485	0.578186	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=354761 Ack=1 Win=66608 Len=1448
486	0.578291	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=337385 Win=65160 Len=0
487	0.578311	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=356209 Ack=1 Win=66608 Len=1448
488	0.578417	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=338833 Win=65160 Len=0
489	0.578436	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=357657 Ack=1 Win=66608 Len=1448
490	0.578541	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=340281 Win=65160 Len=0
491	0.578561	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=359105 Ack=1 Win=66608 Len=1448
492	0.578666	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=341729 Win=65160 Len=0
493	0.578685	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=360553 Ack=1 Win=66608 Len=1448
494	0.578791	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=343177 Win=65160 Len=0
495	0.578810	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=362001 Ack=1 Win=66608 Len=1448
496	0.578916	192.0.0.1	193.0.0.1	TCP	ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=65160 Len=0
497	0.578936	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=363449 Ack=1 Win=66608 Len=1448
498	0.579041	192.0.0.1	193.0.0.1	TCP	[TCP Dup ACK 496#1] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
499	0.597654	192.0.0.1	193.0.0.1	TCP	[TCP Dup ACK 496#2] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
500	0.597673	193.0.0.1	192.0.0.1	TCP	64611 > ndmp [ACK] Seq=364897 Ack=1 Win=66608 Len=1448

```
501 0.597779    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#3] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
502 0.597797    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=366345 Ack=1 Win=66608 Len=1448
503 0.597905    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#4] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
504 0.597907    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#5] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
505 0.597926    193.0.0.1    192.0.0.1    TCP      [TCP Retransmission] 64611 > ndmp [ACK] Seq=344625 Ack=1 Win=66608 Len=1448
506 0.598154    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#6] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
507 0.598156    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#7] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
508 0.598404    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#8] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
509 0.598406    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#9] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
510 0.598529    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#10] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
511 0.598779    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#11] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
512 0.598781    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#12] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
513 0.598904    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#13] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
514 0.598921    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=367793 Ack=1 Win=66608 Len=1448
515 0.617642    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#14] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
516 0.617661    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=369241 Ack=1 Win=66608 Len=1448
517 0.617804    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 496#15] ndmp > 64611 [ACK] Seq=1 Ack=344625 Win=66608 Len=0
518 0.617829    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=370689 Ack=1 Win=66608 Len=1448
519 0.617894    192.0.0.1    193.0.0.1    TCP      ndmp > 64611 [ACK] Seq=1 Ack=367793 Win=43440 Len=0
520 0.617896    192.0.0.1    193.0.0.1    TCP      [TCP Dup ACK 519#1] ndmp > 64611 [ACK] Seq=1 Ack=367793 Win=66608 Len=0
521 0.617921    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=372137 Ack=1 Win=66608 Len=1448
522 0.617931    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=373585 Ack=1 Win=66608 Len=1448
523 0.617941    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=375033 Ack=1 Win=66608 Len=1448
524 0.617965    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=376481 Ack=1 Win=66608 Len=1448
525 0.617985    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=377929 Ack=1 Win=66608 Len=1448
526 0.618023    192.0.0.1    193.0.0.1    TCP      ndmp > 64611 [ACK] Seq=1 Ack=369241 Win=65160 Len=0
527 0.618047    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=379377 Ack=1 Win=66608 Len=1448
528 0.637631    192.0.0.1    193.0.0.1    TCP      ndmp > 64611 [ACK] Seq=1 Ack=370689 Win=65160 Len=0
529 0.637665    193.0.0.1    192.0.0.1    TCP      64611 > ndmp [ACK] Seq=380825 Ack=1 Win=66608 Len=1448
```

Annexe 4 : courbe associée à la capture de l'annexe 3

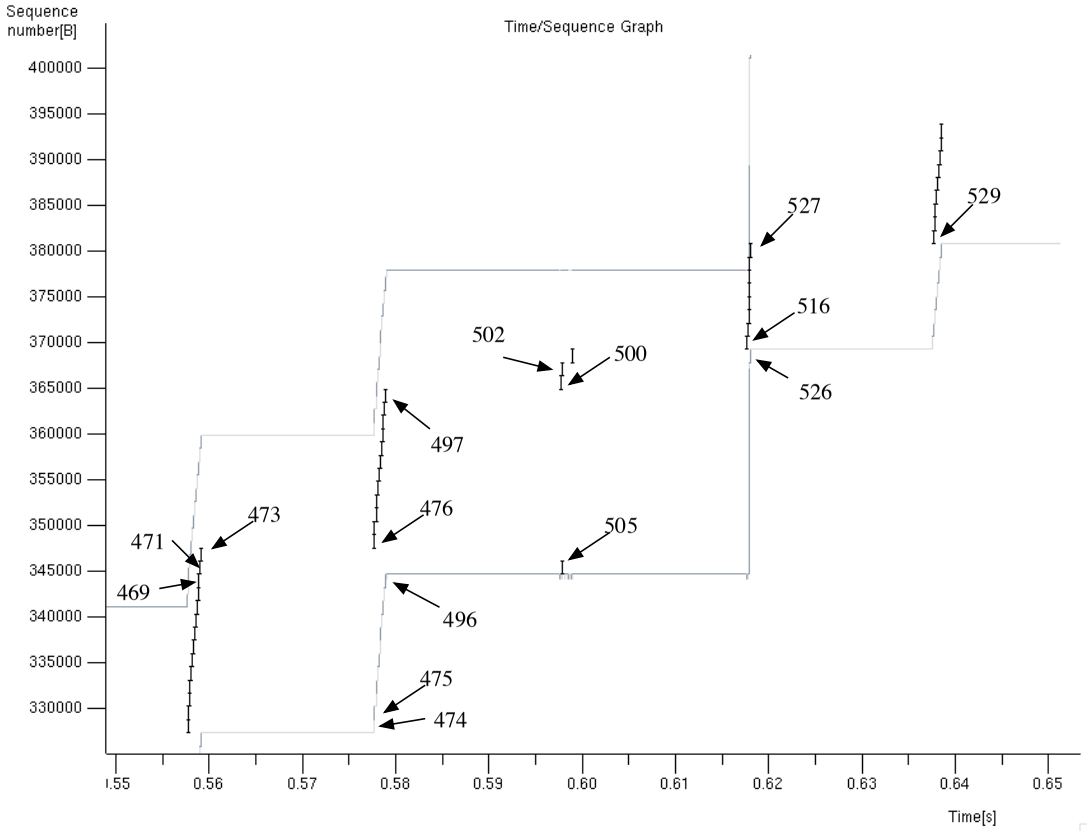

Figure 4 – Evolution des numéros de séquence et d'acquittement