

Examen

Introduction aux réseaux

Master Informatique 1ère année
P. Sicard

8 décembre 2016

Durée : 3 heures

Tous documents autorisés. Ordinateurs interdits.

Un barème approximatif est donné.

1 Protocole transport (10 points)

En annexe 1 sont données les traces de captures de paquets sur un ordinateur. Chaque ligne décrit un paquet. 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 (ici *TCP*),
- puis les valeurs de certains champs de l'entête TCP :
 - des indications sur des fonctionnalités du paquet (par exemple *TCP Dup ACK*)
 - 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 et lors de l'émission de données (de taille importante) à travers cette connexion de la machine d'adresse *192.168.1.1* vers *193.54.236.147*.

La capture a été effectuée sur la machine d'adresse *192.168.1.1*. Le buffer d'émission sur la machine *192.168.1.1* a été fixé à **5792 octets**, le buffer de réception sur la machine *193.54.236.147* a été fixé à **15 000 octets**.

En annexe 3 est donné pour la même capture la courbe d'évolution :

- des numéros de séquence TCP (en traits foncés),
- des numéros d'acquittement TCP (en traits clairs)
- et du dernier numéro de séquence pouvant être réceptionné (valeur du champ WIN de TCP + le numéro d'acquittement).

Le temps sur les abscisses est donné en seconde. Les numéros de paquets sont indiqués sur la courbe.

Les paquets 31 et 32 se superposent sur la courbe.

Répondre de façon précise aux questions suivantes :

1. Le temps d'aller-retour (RTT : Round trip time) entre les deux machines en jeu est de l'ordre de 120 millisecondes. Faites-le apparaître sur la courbe (on pourra rendre l'annexe 3 avec sa copie).

Remarque : Le RTT est constant tout au long de cette capture.

2. Le paquet 16 contient des données (TCP). Combien d'octets ?
3. Le paquet 28 contient-il des données ? A quoi sert-il ? Pourquoi son numéro d'acquittement (relatif) est-il égal à 17376 ? Faites apparaître le paquet sur la courbe de l'annexe 3. Quels paquets acquitte-t-il ?
4. Pourquoi l'émetteur s'arrête-t-il d'émettre pendant 120 ms après les paquets 19-20-23 et 24 ? Retrouvez sur la courbe la taille du buffer d'émission.
5. On se place sur la machine d'adresse *192.168.1.1* après la réception du paquet **28**. Complétez la figure 1 ci-dessous représentant la fenêtre de la récupération d'erreur en faisant apparaître les valeurs des éléments suivants :
 - le numéro du dernier octet acquitté par le récepteur (*Dernier octet acquitté*),
 - la taille du buffer d'émission,
 - le numéro de séquence maximal que l'émetteur a déjà envoyé (*Dernier octet émis*),
 - le numéro de séquence maximal que l'émetteur peut envoyer à ce moment là (*Dernier octet pouvant être émis*).

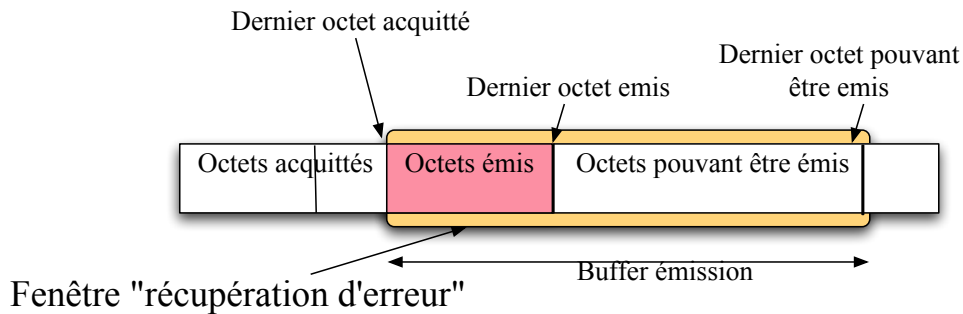


Figure 1 – Fenêtre à anticipation de la récupération d’erreur

6. Après l’envoi du paquet 29 combien d’octets la machine d’adresse *193.54.236.147* peut-elle encore stocker dans son buffer de réception ? Comment le savez vous ?
7. On se place sur la machine d’adresse *192.168.1.1* après la réception du paquet **29**. Complétez la figure 2 ci-dessous représentant la fenêtre du contrôle de flux en faisant apparaître les valeurs des éléments suivants :
 - le numéro du dernier octet acquitté par le récepteur (*Dernier octet acquitté*),
 - la taille du buffer de réception,
 - le numéro de séquence maximal que l’émetteur a déjà envoyé (*Dernier octet émis*),
 - le numéro de séquence maximal que l’émetteur peut envoyer à ce moment là (*Dernier octet pouvant être émis*),
 - le numéro du dernier octet lu par l’application sur le récepteur (*Dernier octet lu*).

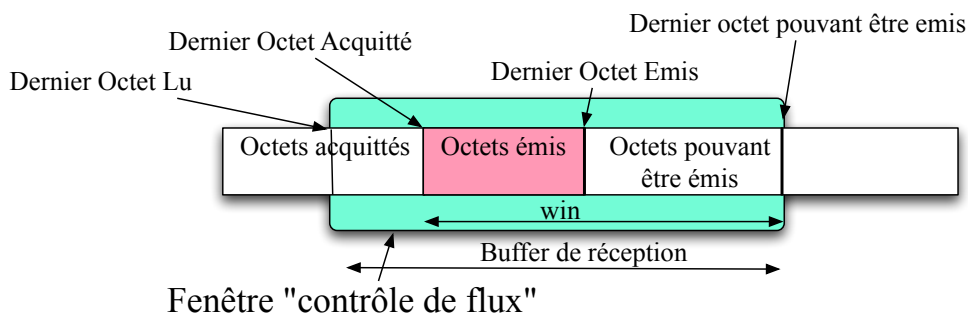


Figure 2 – Fenêtre à anticipation du contrôle de flux

8. Faites apparaître sur la figure 2 la fenêtre de la récupération d’erreur à cet instant. Donnez sa limite inférieure et supérieure.
9. Pourquoi l’émission des données est-elle interrompue pendant un laps de temps important entre le paquet 27 et 32 ? A quoi sert le paquet 31 ? Pourquoi est-il marqué *TCP Dup Ack* par l’outil de capture ? Quelle différence comporte-t-il avec le paquet 30 ? Qu’est ce qui a déclenché son émission ?

10. Pourquoi la courbe *WIN+ Numéro d'acquittement* est elle horizontale du paquet 15 au paquet 31 ?
11. On se place maintenant dans le cas où le récepteur n'est jamais saturé (pas de contrôle de flux nécessaire). En supposant que le débit réel sur les réseaux sur lesquels sont connectées les deux machines est de 10 mégabit/s.
Quel débit peut-on espérer avoir au mieux (pas de perte de paquet) au niveau de l'application utilisant TCP dans cette configuration (RTT constant à 120 ms, buffers d'émission et de réception fixés ainsi). Expliquez en détail vos calculs.
12. Quelle taille minimale des buffers d'émission et de réception faudrait-il utiliser pour obtenir un débit applicatif optimal ? Expliquez en détail vos calculs.
13. Pourquoi est-il inutile d'avoir un buffer d'émission plus grand que le buffer de réception ?

2 Adressage et routage (10 points)

2.1 Questions simples

Voici le résultat de la commande *ifconfig* sur un ordinateur :

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=3<RXCSUM,TXCSUM>
inet6 ::1 prefixlen 128
inet 127.0.0.1 netmask 0xff000000
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
nd6 options=1<PERFORMNUD>

en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=b<RXCSUM,TXCSUM,VLAN_HWTAGGING>
ether c8:bc:c8:92:5d:8d
inet 129.88.48.196 netmask 0xfffffc00 broadcast 129.88.51.255
media: autoselect (100baseTX <full-duplex>)
status: active
```

1. Combien d'interfaces réseaux existe-t-il sur cet ordinateur ? De quel type ? Pourquoi l'adresse IP 127.0.0.1 apparaît-elle ?
2. Expliquez la ligne *ether c8:bc:c8:92:5d:8d*
3. Quelle est l'adresse IP de cet ordinateur ? Quel est le netmask associé à cette adresse IP ? Du coup quelle est la longueur de son préfixe (/x) ?
4. Quelle est l'adresse du réseau auquel appartient cet ordinateur ? Comment l'avez-vous calculé ?
5. Que veut dire *broadcast 129.88.51.255* ? Retrouvez à partir du netmask et de l'adresse IP cette valeur. A quoi sert elle ?

2.2 PLAN D'ADRESSAGE ET ROUTAGE STATIQUE

Vous devez administrer un réseau d'ordinateurs suivant le plan donné dans l'Annexe 3.

- Les deux switches (commutateurs) sont de type Ethernet.
- Le routeur 1 est relié à une ligne téléphonique (protocole ADSL) pour l'accès à Internet. Il possède aussi trois interfaces Ethernet dont une est relié à une borne d'accès WIFI.

- Le routeur 2 possède une interface Ethernet et une interface WIFI (connectée via des ondes radio à la borne WIFI).
- Le routeur 3 possède 2 interfaces Ethernet et une interface WIFI (connectée via des ondes radio à la borne WIFI).
- L'hôte A est connecté à la borne WIFI via des ondes radio grâce à son interface WIFI.
- Les hôtes B,C, D et E sont connectés via leur interface Ethernet.
- Tous les liens apparaissant sur le plan sont en paire torsadée.

Rappel : Une borne WIFI est un pont Ethernet/WIFI, ce n'est donc pas un routeur.

1. L'interface extérieure du routeur 1 (permettant la liaison avec Rext1) est configurée via le protocole DHCP. Le contenu du paquet DHCP-ACK envoyé par un serveur DHCP au routeur 1 est donné dans l'annexe 4. A l'aide de ces informations répondez aux questions suivantes :
 - Donnez l'adresse IP qui sera attribuée à l'interface extérieure du routeur 1. Donnez le nombre de bits de la partie "réseau" de cette adresse.
 - Donnez la table de routage résultante du routeur 1.
 - L'adresse d'un serveur DNS est aussi donné dans le paquet DHCP. Quel inconvénient apparaîtrait si ce n'était pas le cas ?

2. Combien de réseaux apparaissent dans cet Intranet (sans compter le réseau entre *Rout1* et *RExt1*) ? Combien d'adresses IP sont nécessaires sur chacun d'eux ?

3. Proposez un plan d'adressage pour cet Intranet en utilisant la page d'adresse **155.64.64.96/27**. **On n'utilisera pas d'adresses privées**. Expliquez le découpage en sous-réseaux que vous effectuez pour cela.
 Donnez le « Netmask » associé à chacun des sous-réseaux.
Remarque : Vous pouvez rendre l'annexe 3 annotée des adresses des routeurs et des ordinateurs hôtes.

4. Donnez les tables de routage des hôtes A, B, C et E et des trois routeurs *R1*, *R2* et *R3* de telle manière que :
 - Tous les hôtes de l'Intranet communiquent entre eux.
 - Tous les hôtes de l'Intranet peuvent communiquer avec des ordinateurs extérieurs (Internet).
 - Les chemins résultants pour ces communications soient toujours les plus courts (en terme de nombre de réseaux traversés), à l'intérieur de l'Intranet et vers l'extérieur.
 - Les tables de routages possèdent 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 sur le plan d'adressage).

- Attention les routeurs possèdent plusieurs adresses.
- Vous rappellerez les lignes de connexions directes aux réseaux qui apparaissent à l'initialisation des interfaces dans ces tables de routage.

2.3 ROUTAGE AUTOMATIQUE – PROTOCOLE RIP

On vide l'ensemble des tables de routage puis on lance le protocole RIP (version 2) sur les 3 routeurs de l'Intranet et les ordinateurs hôtes. On ne lance pas RIP sur le réseau extérieur.

Remarque : la version 2 du protocole RIP fournit aussi les netmasks associés aux adresses de réseau échangées.

1. Donnez le contenu des tables de routage des routeurs **Rout1** et **Rout3**, et des hôtes **D** et **C**, une fois qu'elles se sont stabilisées (entièrement remplies). Y a-t-il plusieurs solutions ? Pourquoi ?
2. Donnez le contenu des paquets RIP (liste des adresses réseau / netmask / métrique) envoyés alors par le routeur **Rout3** sur les trois réseaux auxquels il est connecté.
3. Les ordinateurs hôtes peuvent-ils accéder à Internet ? Si non que faut-il rajouter aux tables de routage des routeurs et des hôtes pour que les hôtes aient accès à l'Internet ?
4. Le routeur **Rout3** tombe en panne.
 - Donnez la table de routage résultante de l'hôte **D** après quelques minutes.
 - Expliquez en détails ce qu'il s'est passé au niveau du protocole RIP (événements particuliers comme *sonnerie de timer*, *réception/émission de paquet RIP*, *modifications de table de routage ...*) pour arriver à cette nouvelle table de routage.
 - Supposons que l'on fasse un *ping* de D vers C juste après la panne du routeur, pendant combien de temps ce ping n'aura t il pas de réponse ? Expliquez votre réponse.

3 Annexe 1 :

8

<i>No.</i>	<i>Time</i>	<i>Source</i>	<i>Destination</i>	<i>Protocol</i>	<i>Info</i>
15	0.352833	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=10136 Ack=0 Win=33304 Len=1448
16	0.352851	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=11584 Ack=0 Win=33304 Len=1448
17	0.352863	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=8688 Win=12128 Len=0
18	0.472619	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=10136 Win=10680 Len=0
19	0.472699	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=13032 Ack=0 Win=33304 Len=1448
20	0.472719	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=14480 Ack=0 Win=33304 Len=1448
21	0.472734	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=11584 Win=9232 Len=0
22	0.472759	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=13032 Win=7784 Len=0
23	0.472807	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=15928 Ack=0 Win=33304 Len=1448
24	0.472826	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=17376 Ack=0 Win=33304 Len=1448
25	0.592619	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=14480 Win=6336 Len=0
26	0.592689	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=15928 Win=4888 Len=0
27	0.592737	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=18824 Ack=0 Win=33304 Len=1448
28	0.592764	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=17376 Win=3440 Len=0
29	0.592833	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=18824 Win=1992 Len=0
30	0.712640	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=20272 Win=544 Len=0
31	5.392707	193.54.236.147	192.168.1.1	TCP	[TCP Dup ACK 30#1] 55768 > 57041 [ACK] Seq=0 Ack=20272 Win=10544 Len=0
32	5.392839	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=20272 Ack=0 Win=33304 Len=1448
33	5.392856	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=21720 Ack=0 Win=33304 Len=1448
34	5.392874	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=23168 Ack=0 Win=33304 Len=1448
35	5.514987	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=21720 Win=9096 Len=0
36	5.515079	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=24616 Ack=0 Win=33304 Len=1448
37	5.515101	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=26064 Ack=0 Win=33304 Len=1448
38	5.515114	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=23168 Win=7648 Len=0
39	5.515138	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=24616 Win=6200 Len=0
40	5.515184	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [ACK] Seq=27512 Ack=0 Win=33304 Len=1448
41	5.515204	192.168.1.1	193.54.236.147	TCP	57041 > 55768 [PSH, ACK] Seq=28960 Ack=0 Win=33304 Len=1448
42	5.632693	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=26064 Win=4752 Len=0
43	5.632766	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=27512 Win=3304 Len=0
44	5.632839	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=28960 Win=1856 Len=0
45	5.632910	193.54.236.147	192.168.1.1	TCP	55768 > 57041 [ACK] Seq=0 Ack=30408 Win=408 Len=0

4 Annexe 2

6

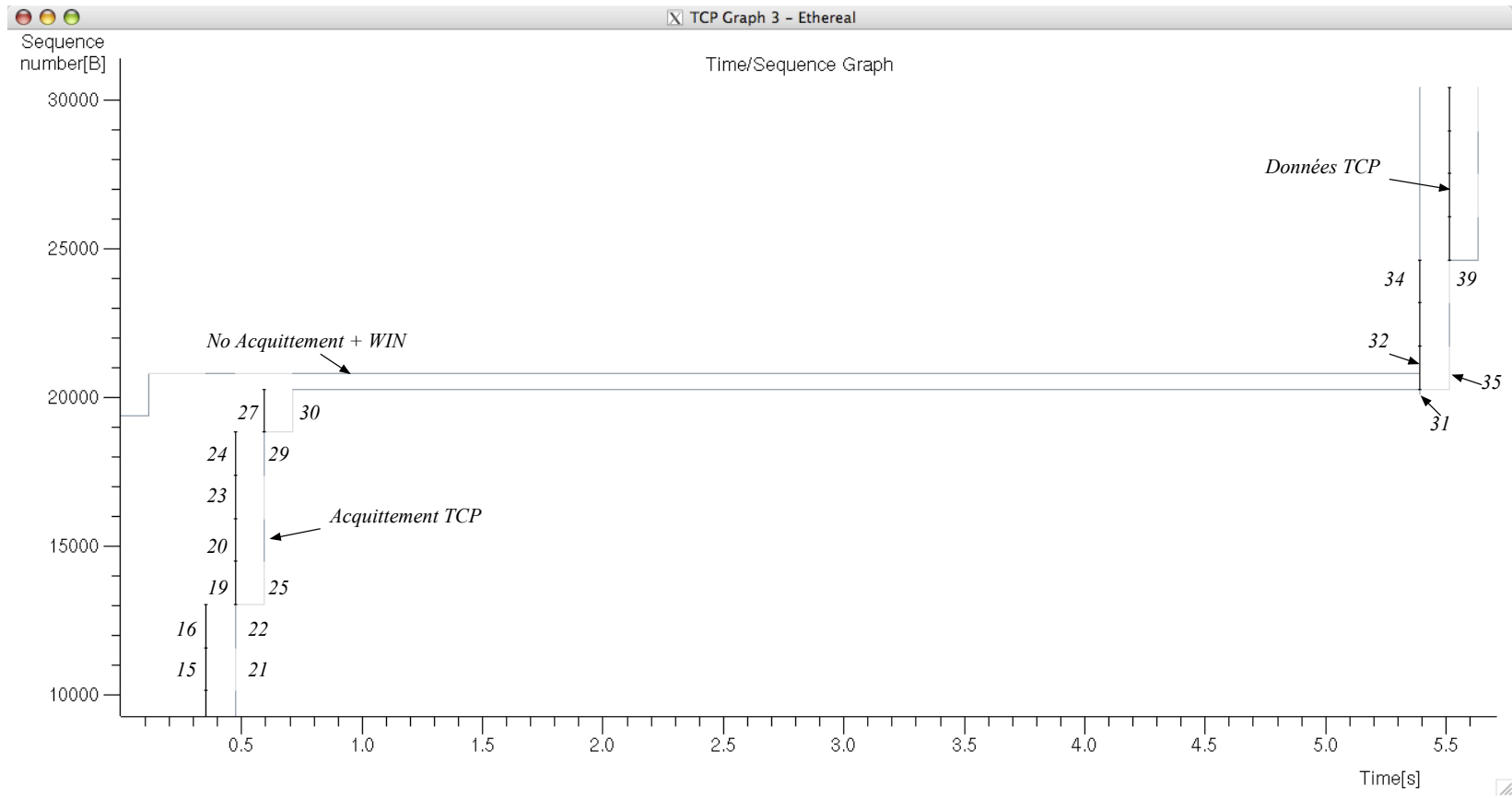


Figure 3 – Courbe d'évolution des numéros de séquences, des numéros d'acquittements et de la fenêtre de réception WIN

5 Annexe 3

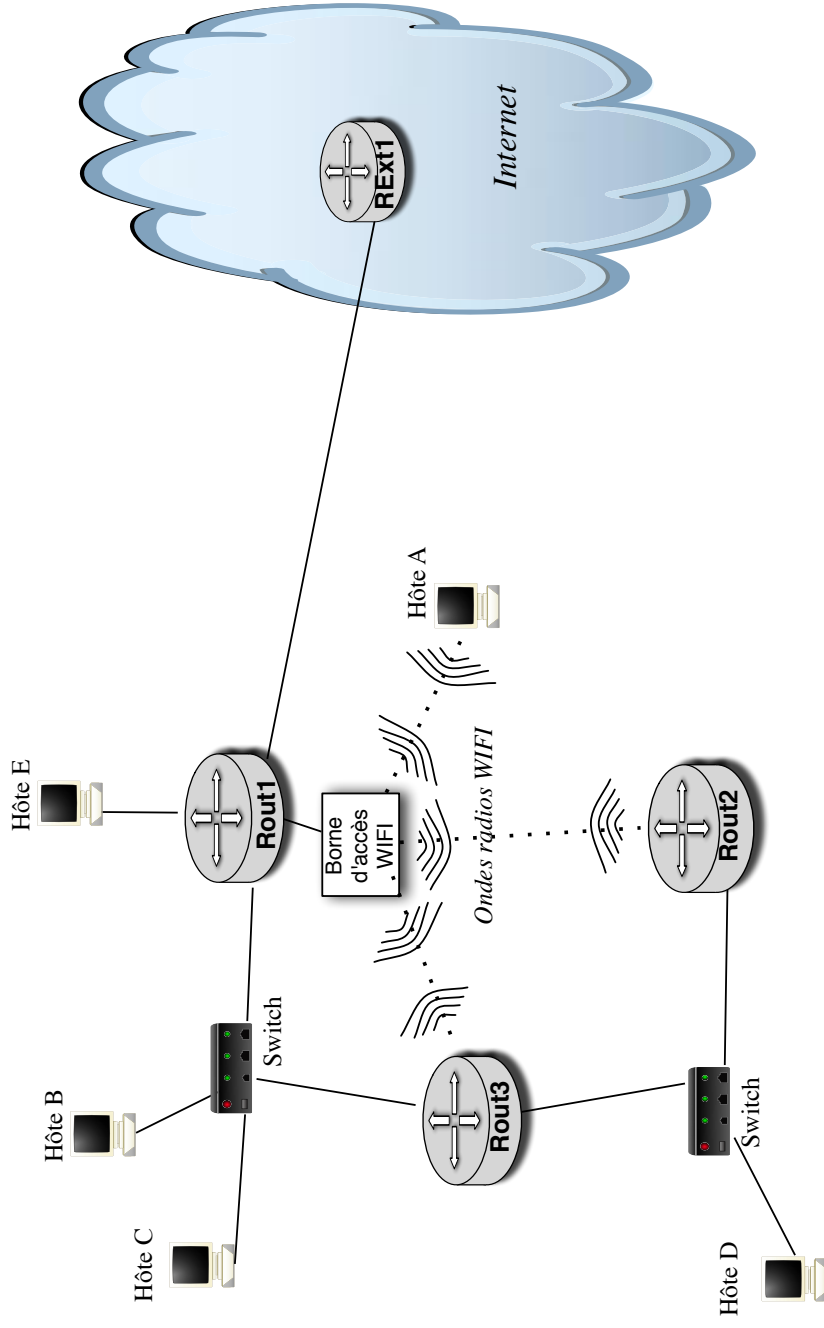


Figure 4 – Topologie du réseau à administrer

