

Corrigé du TP 6 Réseaux

Commandes et applications réseau (DNS, TELNET, FTP, SMTP, POP3) et simulation Nat/Pat/Firewall

C. Pain-Barre

INFO - IUT Aix-en-Provence

version du 6/4/2011

1 Commandes réseau

1.1 Commande netstat

Corrigé de l'exercice 1 (netstat sur allegro)

[\[Consulter l'énoncé\]](#)

1. `netstat -a`

⇒ on n'obtient pas cependant la table de routage de allegro, mais on aura les informations sur les serveurs en attente de requêtes, les connexions ouvertes, les ports TCP et UDP utilisés, etc. Notons que concernant TCP (ou UDP), les extrémités sont notées *adresse : port*

2. `netstat -r`

⇒ cela revient à taper : `route`

3. `netstat -nr`

4. `netstat -t` ou `netstat --tcp`

⇒ cette option n'est pas vraiment documentée mais apparaît dans le synopsis



En revanche, `netstat -tcp` serait la même chose que `netstat -t -c -p...`

Corrigé de l'exercice 2 (netstat sur windows)

[\[Consulter l'énoncé\]](#)

1. `netstat -a`

2. `netstat -r`

3. `netstat -p TCP`

2 Noms de stations et de domaine

2.1 Noms officiels

2.1.1 Sous Unix

Corrigé de l'exercice 3 (noms officiels sur allegro)

[\[Consulter l'énoncé\]](#)

1. `cat /etc/hosts` affiche :

```
127.0.0.1          localhost
139.124.187.4     allegro.iut.univ-aix.fr allegro
```

↪ ainsi, allegro ne reconnaît que des noms officiels qui concernent ses propres adresses

2. `cat /etc/networks` affiche :

```
default          0.0.0.0
loopback         127.0.0.0
link-local       169.254.0.0
```

link-local correspond à un réseau privé (auto-configuration d'adresse IP privée en cas d'absence d'un serveur DHCP pour une station qui en a besoin)

2.1.2 Sous Windows

Corrigé de l'exercice 4 (noms officiels sur windows)

[\[Consulter l'énoncé\]](#)

1. bien souvent, il n'y a que localhost pour 127.0.0.1
2. bien souvent, il n'y a que loopback pour 127.0.0.0

2.2 Noms officiels

2.2.1 Commande hostname

Corrigé de l'exercice 5 (hostname sur allegro)

[\[Consulter l'énoncé\]](#)

1. `hostname -f` ou `hostname --fqdn` ou `hostname --long`
2. `hostname -s` mais `hostname` seule peut suffire aussi
3. `hostname -d`

Corrigé de l'exercice 6 (hostname sur windows)

[\[Consulter l'énoncé\]](#)

`hostname` seul.

2.2.2 Résolution de nom sous Unix et le fichier nsswitch.conf

Corrigé de l'exercice 7 (consultation de /etc/nsswitch.conf sur allegro)

[\[Consulter l'énoncé\]](#)

La ligne :

```
hosts:      files dns wins
```

nous apprend que la résolution consiste d'abord à consulter le fichier `/etc/hosts` puis à réaliser des requêtes DNS et enfin à demander aux serveurs de noms Windows du réseau local

2.2.3 Configuration DNS

Corrigé de l'exercice 8 (consultation de /etc/resolv.conf sur allegro)

[\[Consulter l'énoncé\]](#)

1. La ligne :

```
domain iut.univ-aix.fr
```

indique qu'un nom court tel que `infodoc` sera traité comme le FQDN `infodoc.iut.univ-aix.fr`.

2. il y en a 3 par ordre de préférence : 139.124.187.10, 139.124.1.2 et 139.124.187.3

2.2.4 Interrogation du DNS avec host, dig et nslookup

Corrigé de l'exercice 9 (interrogations DNS sur Linux)

[\[Consulter l'énoncé\]](#)

1. `$ host -t A www.lsis.org`

```
www.lsis.org has address 194.167.251.80
```

⇒ *a priori*, il n'est pas nécessaire de préciser l'option `-t A` qui devrait être prise par défaut.

2. `$ host -t ns lsis.org`

```
lsis.org name server md000u14.u-3mrs.fr.  
lsis.org name server esm2.imt-mrs.fr.  
lsis.org name server lsis-dns.lsis.org.  
lsis.org name server lsis-gateway.lsis.org.
```

⇒ il y a donc 4 serveurs de noms pour ce domaine.

3. `$ dig univmed.fr MX`

```
; <<>> DiG 9.3.1 <<>> univmed.fr MX  
;; global options: printcmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 11286  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5  
  
;; QUESTION SECTION:
```

```

;univmed.fr.                IN      MX

;; ANSWER SECTION:
univmed.fr.                3600   IN      MX      0 mx0.univmed.fr.
univmed.fr.                3600   IN      MX      10 smtp.univmed.fr.

;; AUTHORITY SECTION:
univmed.fr.                39132  IN      NS      romarin.univ-aix.fr.
univmed.fr.                39132  IN      NS      riluminy.univ-mrs.fr.
univmed.fr.                39132  IN      NS      cnudns.cines.fr.

;; ADDITIONAL SECTION:
mx0.univmed.fr.            86400  IN      A       139.124.132.122
smtp.univmed.fr.           39143  IN      A       139.124.132.120
romarin.univ-aix.fr.       39132  IN      A       193.50.125.2
riluminy.univ-mrs.fr.      39132  IN      A       139.124.1.2
riluminy.univ-mrs.fr.      39132  IN      AAAA    2001:660:5402:801::2

;; Query time: 3 msec
;; SERVER: 139.124.187.10#53 (139.124.187.10)
;; WHEN: Tue May 13 05:40:05 2008
;; MSG SIZE rcvd: 251

```

⇨ **dig** est assez bavard et nous indique plusieurs renseignements :

- il y a 2 serveurs de mail (SMTP) indiqués dans la section réponse (ANSWER) : `mx0.univmed.fr` et `smtp.univmed.fr`. Celui à préférer est `mx0.univmed.fr` car sa priorité est 0
- les serveurs de noms faisant autorité sur le domaine interrogé sont `romarin.univ-aix.fr`, `riluminy.univ-mrs.fr` et `cnudns.cines.fr`
- les adresses de quelques uns de ces serveurs (enregistrements de type A) sont indiqués dans la section additionnelle. L'enregistrement de type AAAA correspond à une adresse IPv6

4. \$ nslookup

```

> set norec
> set q=ns
> pasteur.fr.
Server:                139.124.187.10
Address:                139.124.187.10#53

```

```

Non-authoritative answer:
*** Can't find pasteur.fr.: No answer

```

Authoritative answers can be found from:

```

fr      nameserver = D.EXT.NIC.fr.
fr      nameserver = G.EXT.NIC.fr.
fr      nameserver = C.NIC.fr.
fr      nameserver = B.EXT.NIC.fr.
fr      nameserver = F.EXT.NIC.fr.
fr      nameserver = A.NIC.fr.
fr      nameserver = E.EXT.NIC.fr.
fr      nameserver = E.NIC.fr.

```

```
A.NIC.fr      internet address = 192.93.0.129
A.NIC.fr      has AAAA address 2001:660:3005:3::1:1
```

⇒ comme prévu (si personne n'a fait d'erreur), notre serveur de noms ne sait pas répondre mais nous indique qu'on peut passer par un serveur de noms du domaine **.fr**. On prend alors le serveur 192.93.0.129 (A.NIC.fr) qui nous est proposé

```
> server 192.93.0.129
Default server: 192.93.0.129
Address: 192.93.0.129#53
> pasteur.fr.
Server:      192.93.0.129
Address:     192.93.0.129#53
```

```
Non-authoritative answer:
*** Can't find pasteur.fr.: No answer
```

```
Authoritative answers can be found from:
pasteur.fr      nameserver = ns1.pasteur.fr.
pasteur.fr      nameserver = ns0.pasteur.fr.
ns0.pasteur.fr  internet address = 157.99.64.64
ns1.pasteur.fr  internet address = 157.99.64.65
```

⇒ on apprend qu'a priori les serveurs de noms de ce domaine sont 157.99.64.64 (ns0.pasteur.fr) et 157.99.64.65 (ns1.pasteur.fr) mais on va vérifier auprès de l'un d'eux car le serveur interrogé ne fait pas autorité

```
> server 157.99.64.64
Default server: 157.99.64.64
Address: 157.99.64.64#53
> pasteur.fr.
Server:      157.99.64.64
Address:     157.99.64.64#53
```

```
pasteur.fr      nameserver = ns0.pasteur.fr.
pasteur.fr      nameserver = ns1.pasteur.fr.
```

⇒ cette fois la réponse est ferme. On peut vérifier l'adresse de ns0.pasteur.fr :

```
> set q=A
> ns0.pasteur.fr.
Server:      157.99.64.64
Address:     157.99.64.64#53
```

```
Name:  ns0.pasteur.fr
Address: 157.99.64.64
```

⇒ plus aucun doute sur l'adresse du serveur de noms.

```
> set q=mx
> pasteur.fr.
Server:      157.99.64.64
```

```
Address:          157.99.64.64#53

pasteur.fr       mail exchanger = 0 mail1.pasteur.fr.
pasteur.fr       mail exchanger = 10 mail0.pasteur.fr.
```

⇒ il y a 2 mail exchangers : mail1.pasteur.fr à utiliser par défaut (priorité 0) et mail0.pasteur.fr à utiliser en second ressort (priorité 10). Il nous manque l'adresse de mail1.pasteur.fr :

```
> set q=a
> mail1.pasteur.fr.
Server:          157.99.64.64
Address:         157.99.64.64#53
```

```
Name:   mail1.pasteur.fr
Address: 157.99.64.73
```

⇒ 157.99.64.73 est son adresse

```
> exit
```

Corrigé de l'exercice 10 (interrogations DNS sur Windows)

[\[Consulter l'énoncé\]](#)

```
Z:\>nslookup
```

```
Serveur par défaut : paprika.iut.univ-aix.fr
Address: 139.124.187.10
```

```
> set norecurse
```

```
> set type=NS
```

```
> pasteur.fr.
```

```
Serveur : paprika.iut.univ-aix.fr
Address: 139.124.187.10
```

```
fr      nameserver = e.ext.NIC.fr
```

```
fr      nameserver = f.ext.NIC.fr
```

```
fr      nameserver = e.NIC.fr
```

```
fr      nameserver = c.NIC.fr
```

```
fr      nameserver = d.ext.NIC.fr
```

```
fr      nameserver = b.ext.NIC.fr
```

```
fr      nameserver = g.ext.NIC.fr
```

```
fr      nameserver = a.NIC.fr
```

```
a.NIC.fr      internet address = 192.93.0.129
```

```
a.NIC.fr      AAAA IPv6 address = 2001:660:3005:3:0:0:1:1
```

```
e.NIC.fr      internet address = 194.57.253.1
```

```
> server 192.93.0.129
```

```
Serveur par défaut : a.nic.fr
```

```
Address: 192.93.0.129
```

```
> pasteur.fr.
```

```
Serveur : a.nic.fr
```

```
Address: 192.93.0.129
```

```
pasteur.fr      nameserver = ns0.pasteur.fr
pasteur.fr      nameserver = ns1.pasteur.fr
ns0.pasteur.fr  internet address = 157.99.64.64
ns1.pasteur.fr  internet address = 157.99.64.65
```

> **server 157.99.64.64**

```
(root) nameserver = D.ROOT-SERVERS.NET
(root) nameserver = E.ROOT-SERVERS.NET
(root) nameserver = F.ROOT-SERVERS.NET
(root) nameserver = G.ROOT-SERVERS.NET
(root) nameserver = H.ROOT-SERVERS.NET
(root) nameserver = I.ROOT-SERVERS.NET
(root) nameserver = J.ROOT-SERVERS.NET
(root) nameserver = K.ROOT-SERVERS.NET
(root) nameserver = L.ROOT-SERVERS.NET
(root) nameserver = M.ROOT-SERVERS.NET
(root) nameserver = A.ROOT-SERVERS.NET
(root) nameserver = B.ROOT-SERVERS.NET
(root) nameserver = C.ROOT-SERVERS.NET
Serveur par défaut : [157.99.64.64]
Address: 157.99.64.64
```

> **pasteur.fr.**

```
Serveur : [157.99.64.64]
Address: 157.99.64.64
```

```
pasteur.fr      nameserver = ns0.pasteur.fr
pasteur.fr      nameserver = ns1.pasteur.fr
ns0.pasteur.fr  internet address = 157.99.64.64
ns1.pasteur.fr  internet address = 157.99.64.65
```

> **set type=MX**

> **pasteur.fr.**

```
Serveur : [157.99.64.64]
Address: 157.99.64.64
```

```
pasteur.fr      MX preference = 10, mail exchanger = mail0.pasteur.fr
pasteur.fr      MX preference = 0, mail exchanger = mail1.pasteur.fr
pasteur.fr      nameserver = ns1.pasteur.fr
pasteur.fr      nameserver = ns0.pasteur.fr
mail1.pasteur.fr internet address = 157.99.64.73
mail0.pasteur.fr internet address = 157.99.64.72
ns0.pasteur.fr  internet address = 157.99.64.64
ns1.pasteur.fr  internet address = 157.99.64.65
```

> **set type=A**

> **mail1.pasteur.fr.**

```
Serveur : [157.99.64.64]
Address: 157.99.64.64
```

```
Nom : mail1.pasteur.fr
Address: 157.99.64.73
```

> **exit**

2.2.5 WHOIS : informations sur les gestionnaires d'un domaine

Corrigé de l'exercice 11 (interrogation whois sur Linux)

[\[Consulter l'énoncé\]](#)

```
$ whois univ-aix.fr
...
$ whois univ-mrs.fr
...
$ whois free.fr
...
...
```

3 TELNET

3.1 Terminal virtuel

Corrigé de l'exercice 12 (Utilisation de telnet depuis Linux)

[\[Consulter l'énoncé\]](#)

1. `$ telnet allegro`
Trying 139.124.187.4...
Connected to allegro.iut.univ-aix.fr.
Escape character is '^]'.
Debian GNU/Linux lenny/sid
allegro login:
2. allegro login: **cpb**
Password: **mot de passe caché**
3. `$ ls -l`
total 1760
drwx----- 5 cpb prof 4096 mai 21 2008 Desktop
drwx----- 2 cpb prof 4096 mai 21 2008 Documents
drwx----- 4 cpb prof 4096 jui 10 2008 GNUstep
drwx----- 2 cpb prof 4096 mai 21 2008 Groupe
drwx----- 2 cpb prof 4096 mai 21 2008 Images
drwx----- 2 cpb prof 4096 mai 21 2008 mail
-rw----- 1 cpb prof 1430186 sep 24 2007 mbox
drwx----- 40 cpb prof 4096 fév 16 17:02 personnel
drwxr-xr-x 15 cpb prof 4096 mai 21 2008 public
drwxr-x--- 2 cpb daemon 4096 mai 21 2008 public_html
-rwx----- 1 cpb prof 600 août 25 2008 PUTTY.RND
drwxr--r-- 2 cpb prof 4096 mai 21 2008 rfc
-rw-r--r-- 1 cpb prof 47018 mar 28 2007 rfc1939.txt
-rw-r--r-- 1 cpb prof 120432 mar 28 2007 rfc821
-rw-r--r-- 1 cpb prof 124482 mai 13 2008 rfc821.txt
drwx----- 4 cpb prof 4096 mai 21 2008 tmp
drwx----- 11 cpb prof 4096 mai 21 2008 tp
drwx----- 4 cpb prof 4096 mai 21 2008 tpres

4. \$ **Alt**+**Ctrl**+**J**

telnet>

5. telnet> **help**

Commands may be abbreviated. Commands are:

close	close current connection
logout	forcibly logout remote user and close the connection
display	display operating parameters
mode	try to enter line or character mode ('mode ?' for more)
open	connect to a site
quit	exit telnet
send	transmit special characters ('send ?' for more)
set	set operating parameters ('set ?' for more)
unset	unset operating parameters ('unset ?' for more)
status	print status information
toggle	toggle operating parameters ('toggle ?' for more)
slc	set treatment of special characters

z suspend telnet

environ change environment variables ('environ ?' for more)

telnet>

6. telnet> **Entrée**

Entrée

7. \$ **pwd**

/users/prof/cpb

8. \$ **exit**

logout

Connection closed by foreign host.

\$

Corrigé de l'exercice 13 (Utilisation de telnet depuis Windows)

[\[Consulter l'énoncé\]](#)

1. Z:\>**telnet**

Microsoft (R) Windows 2000 (TM) version 5.00 (numéro 2195)

Client Telnet Microsoft

Client Telnet numéro 5.00.99206.1

Le caractère d'échappement est 'CTRL+\$'

Microsoft Telnet>

2. Microsoft Telnet> **help**

Les commandes peuvent être abrégées. Les commandes prises en charge sont :

close	ferme la connexion en cours
display	affiche les paramètres d'opération
open	ouvre une connexion à un site
quit	quitte telnet
set	définit les options (entrez 'set ?' pour afficher la liste)
status	affiche les informations d'état

```
unset          annule les options (entrez 'unset ?' pour afficher la liste)
? ou help      affiche des informations d'aide
Microsoft Telnet>
```

3. Microsoft Telnet> **open allegro**

```
Debian GNU/Linux lenny/sid
allegro login:
```

4. allegro login: **cpb**

```
Password: mot de passe caché
```

```
Last login: Mon Apr  6 10:41:41 CEST 2009 from b100.iut.univ-aix.fr on pts/10
Linux allegro 2.6.26-1-686-bigmem #1 SMP Mon Dec 15 18:58:47 UTC 2008 i686
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
cpb@allegro:~$
```

5. cpb@allegro:~\$ **pwd**

```
/users/prof/cpb
```

```
cpb@allegro:~$ cd public
```

```
cpb@allegro:~/public$ ls
```

```
andreas  checksum      firefox_ie.jpg          share          unix
bin      dataglu       Firefox_wallpaper.png  split          viewdtg
boxes    debian-bin    lanceur_xming          ssh-family    visucodages
chat     figlet        man                    tpres
```

```
cpb@allegro:~/public$
```

6. cpb@allegro:~/public\$ **Ctrl+\$**

```
Microsoft Telnet>
```

7. Microsoft Telnet> **set ?**

```
NTLM          Active l'authentification NTLM.
LOCAL_ECHO    Active l'écho local.
TERM x        (où x est ANSI, VT100, VT52 ou VTNT))
CRLF          Envoi de CR et de LF
```

```
Microsoft Telnet>
```

8. Microsoft Telnet> **set LOCAL_ECHO**

```
Microsoft Telnet>
```

9. Microsoft Telnet> Entrée

```
cpb@allegro:~/public$
```

10. cpb@allegro:~/public\$ **ppwdd**

```
/users/prof/cpb/public
```

```
cpb@allegro:~/public$ ccdd
```

```
cpb@allegro:~$ llss
```

```
Desktop      Groupe  mbox      public_html  rfc1939.txt  tmp
Documents    Images  personnel  PUTTY.RND    rfc821       tp
GNUstep      mail    public     rfc          rfc821.txt   tpres
cpb@allegro:~$
```

```
11. cpb@allegro:~$ eexxiitt
```

```
logout
```

```
Perte de la connexion à l'hôte.
```

```
Appuyez sur une touche pour continuer...
```

```
Microsoft Telnet> quit
```

```
Z:\>
```

3.2 Telnet comme simple client TCP

Corrigé de l'exercice 14 (Utilisation de telnet en client TCP)

[\[Consulter l'énoncé\]](#)

```
1. $ telnet infodoc 13      ou      telnet infodoc daytime
```

```
Trying 139.124.187.14...
```

```
Connected to infodoc.iut.univ-aix.fr.
```

```
Escape character is '^]'.  
06 APR 2009 10:20:02 CEST
```

```
Connection closed by foreign host.
```

↔ la date renvoyée est 06 APR 2009 10:20:02 CEST

```
$ telnet allegro 13
```

```
Trying 139.124.187.4...
```

```
Connected to allegro.iut.univ-aix.fr.
```

```
Escape character is '^]'.  
06 APR 2009 10:25:16 CEST
```

```
Connection closed by foreign host.
```

↔ la date renvoyée est 06 APR 2009 10:25:16 CEST

Les machines oralinux et paprika sont injoignables, ne répondent pas ou refusent le service

```
2. $ telnet infodoc 7      ou      telnet infodoc echo
```

```
Trying 139.124.187.14...
```

```
Connected to infodoc.iut.univ-aix.fr.
```

```
Escape character is '^]'.  
blablabla
```

```
blablabla
```

```
patati
```

```
patati
```

```
et patata
```

```
et patata
```

```
^]
```

```
telnet> close
```

```
Connection closed.
```

```
$
```

4 nmap : scanner un réseau

Corrigé de l'exercice 15 (Utilisation de nmap sur Linux)

[\[Consulter l'énoncé\]](#)

1. \$ nmap allegro

```
Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 10:56 CEST
Interesting ports on allegro.iut.univ-aix.fr (139.124.187.4):
Not shown: 1701 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
13/tcp    open  daytime
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
1521/tcp  open  oracle
2049/tcp  open  nfs
9102/tcp  open  jetdirect
```

Nmap done: 1 IP address (1 host up) scanned in 0.110 seconds

On compare avec ce qu'écrit **netstat -atn** exécutée sur allegro :

```
cpb@allegro:~$ netstat -atn | grep -i listen
tcp        0      0 0.0.0.0:2049          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:54691         0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:7            0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:13           0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:110          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:9102         0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:111          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:1521          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:3090          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:24308         0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:22           0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:631          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:23           0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:22777         0.0.0.0:*           LISTEN
tcp6       0      0 :::139               :::*                LISTEN
tcp6       0      0 :::80                :::*                LISTEN
tcp6       0      0 :::21                :::*                LISTEN
tcp6       0      0 :::22                :::*                LISTEN
tcp6       0      0 :::631               :::*                LISTEN
tcp6       0      0 :::445               :::*                LISTEN
```

- ⇒ Les 6 dernières lignes correspondent à des services utilisant IPv6. La différence avec l'affichage de **nmap** s'explique par le fait que **nmap** ne scanne que les 1024 premiers ports ainsi que ceux indiqués dans un fichier de configuration (actuellement `/usr/share/nmap/nmap-services`). Pour obtenir un scan sur la totalité des ports, il faut taper : **nmap -p 1-65535 allegro**. De plus, **nmap** ne peut pas atteindre les serveurs en attente de connexion sur une adresse de reboilage (notamment ceux utilisant l'adresse 127.0.0.1)

2. \$ nmap infodoc

```
Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 10:59 CEST
Interesting ports on infodoc.iut.univ-aix.fr (139.124.187.14):
Not shown: 1697 closed ports
PORT      STATE SERVICE
7/tcp    open  echo
13/tcp   open  daytime
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
631/tcp  open  ipp
669/tcp  open  unknown
685/tcp  open  unknown
746/tcp  open  unknown
1024/tcp open  kdm
2049/tcp open  nfs
6000/tcp open  X11
9102/tcp open  jetdirect

Nmap done: 1 IP address (1 host up) scanned in 0.106 seconds
```

5 netcat : un client/serveur à tester

Corrigé de l'exercice 16 (Utilisation de netcat sur Linux)

[\[Consulter l'énoncé\]](#)

1. \$ **nc infodoc 13**
06 APR 2009 11:02:43 CEST
\$
2. \$ **nc -u infodoc echo**
blablabla
blablabla
et encore patata
et encore patata
Ctrl+C
\$

3. Voici côte-à-côte ce qui se passe sur les deux terminaux dans le temps :

```
$ nc -l -p 12345
```

```
hello
```

```
qui t'es toi ?
```

```
le pape
```

```
Ctrl+C
```

```
$
```

```
$ telnet localhost 12345
```

```
Trying 127.0.0.1...
```

```
Connected to allegro (127.0.0.1).
```

```
Escape character is '^]'.  
hello
```

```
qui t'es toi ?
```

```
le pape
```

```
Connection closed by foreign host.
```

```
$
```

4. \$ nc -l -u -p 23456

```
salut
```

```
et toi ? qui t'es ?
```

```
ben, encore le pape
```

```
Ctrl+C
```

```
$
```

```
$ nc -u localhost 23456
```

```
salut
```

```
et toi ? qui t'es ?
```

```
ben, encore le pape
```

```
t'es encore là ?
```

```
$
```

⇒ ici, le dialogue utilisant UDP (donc un mode non connecté), **nc** ne détecte qu'il n'y a plus personne à "l'autre bout" que lorsqu'il tente de lui envoyer un message (ce qui le fait recevoir en retour une erreur ICMP de port inatteignable).

6 FTP

6.5 Exercices

Corrigé de l'exercice 17 (Session FTP avec ftp.rfc-editor.org depuis Linux)

[\[Consulter l'énoncé\]](#)

```
$ ftp ftp.rfc-editor.org
Connected to ftp.rfc-editor.org.
220 ftp.isi.edu NcFTPd Server (free educational license) ready.
500 Syntax error, command unrecognized.
Name (ftp.rfc-editor.org:cpb): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password: cyril.pain-barre@univmed.fr
230-You are user #14 of 550 simultaneous users allowed.
230-
230-If you have problems downloading and are seeing "Access denied" or
230-"Permission denied", please make sure that you started your FTP client in
230-a directory to which you have write permission.
230-
230-If your FTP client crashes or hangs shortly after login please try using
```

```

230-a dash (-) as the first character of your password. This will turn off
230-the informational messages that may be confusing your FTP client.
230-
230-All transfers and commands to and from this host are logged.
230-
230-If you experience any problems using ftp, please report them via
230-e-mail to Action@isi.edu.
230-
230 Logged in anonymously.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd in-notes
250-"/in-notes" is new cwd.
250-
250-*=====*
250-* *
250-* This directory is maintained by the RFC Editor. If you experience *
250-* any problems, please report them to rfc-editor@rfc-editor.org. *
250-* *
250-*=====*
250
ftp> passive
Passive mode on.
ftp> ascii
200 Type okay.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> get rfc1939.txt
local: rfc1939.txt remote: rfc1939.txt
227 Entering Passive Mode (128,9,176,20,224,131)
150 Data connection accepted from 139.124.187.4:51543; transfer starting for rfc1939.txt (47018 bytes).
#####
226 Transfer completed.
48309 bytes received in 0.61 seconds (77 Kbytes/s)
ftp> by
221 Goodbye.

```

Corrigé de l'exercice 18 (Dépot d'un fichier sur un serveur FTP)

[\[Consulter l'énoncé\]](#)

1. ... pas besoin de corrigé pour cette question ...
2. Z:> C:
C:> **cd "\Documents And Settings\cpb\Bureau"**
3. C:\Documents and Settings\cpb\Bureau>**ftp allegro**
Connecté à allegro.iut.univ-aix.fr.
220 allegro.iut.univ-aix.fr FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Utilisateur (allegro.iut.univ-aix.fr:(none)) : **cpb**
331 Password required for cpb.
Mot de passe : **mon mot de passe**
230- Linux allegro 2.6.26-1-686-bigmem #1 SMP Mon Dec 15 18:58:47 UTC 2008 i686
230-
230- The programs included with the Debian GNU/Linux system are free software;
230- the exact distribution terms for each program are described in the
230- individual files in /usr/share/doc/*/copyright.
230-
230- Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
230- permitted by applicable law.
230 User cpb logged in.
ftp> **mkdir rfc**
257 "rfc" directory created.
ftp> **cd rfc**

```
250 CWD command successful.
ftp> ascii
200 Type set to A.
ftp> put rfc1939.txt
200 PORT command successful.
150 Opening ASCII mode data connection for 'rfc1939.txt'.
226- WARNING! 1291 bare linefeeds received in ASCII mode
      File may not have transferred correctly.
226 Transfer complete.
ftp : 47018 octets reçus dans 0,00Secondes 47018000,00Ko/sec.
ftp> by
221 Goodbye.
```

```
C:\Documents and Settings\cpb\Bureau>
```

Corrigé de l'exercice 19 (Utilisation de gftp depuis Linux)

[\[Consulter l'énoncé\]](#)

Cet exercice ne devrait pas poser de problèmes particuliers, d'autant qu'en principe **gftp** est déjà configuré pour activer le mode passif. Sinon, il faut le faire à partir du menu *FTP* → *Options*. Sinon, il faut juste penser à mettre *anonymous* comme nom d'utilisateur.

6.6 Messages du protocole FTP

6.7 Exercices

Corrigé de l'exercice 20 (Transfert manuel en mode actif)

[\[Consulter l'énoncé\]](#)

1. `$ telnet allegro 21`
Trying 139.124.187.4...
Connected to allegro.iut.univ-aix.fr (139.124.187.4).
Escape character is '^]'.
220----- Welcome to Pure-FTPd -----
220-You are user number 1 of 50 allowed.
220-Local time is now 12:25. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
2. **USER cpb**
331 User cpb OK. Password required
PASS mon-mot-de-passe
230-User cpb has group access to: prof
230 OK. Current restricted directory is /
3. `$ nc -l -p 12345`
4. **PORT 139,124,187,4,48,57**
200 PORT command successful
5. **LIST**
150 Connecting to port 12345

⇒ ici, allegro envoie le contenu du répertoire sur la connexion avec **nc**

```
226-Options: -a -l
226 81 matches total
```

6. QUIT

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
Connection closed by foreign host.
$
```

Corrigé de l'exercice 21 (Transfert manuel en mode passif)

[\[Consulter l'énoncé\]](#)

```
$ telnet ftp.rfc-editor.org 21
Trying 128.9.176.20...
Connected to ftp.rfc-editor.org (128.9.176.20).
Escape character is '^]'.
220 ftp.isi.edu NcFTPD Server (free educational license) ready.
USER anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS cyril.pain-barre@univmed.fr
230-You are user #41 of 550 simultaneous users allowed.
230-
230-If you have problems downloading and are seeing "Access denied" or
230-"Permission denied", please make sure that you started your FTP client in
230-a directory to which you have write permission.
230-
230-If your FTP client crashes or hangs shortly after login please try using
230-a dash (-) as the first character of your password. This will turn off
230-the informational messages that may be confusing your FTP client.
230-
230-All transfers and commands to and from this host are logged.
230-
230-If you experience any problems using ftp, please report them via
230-e-mail to Action@isi.edu.
230-
230 Logged in anonymously.
CWD in-notes
250-"/in-notes" is new cwd.
250-
250-*=====*
250-*                                     *
250-* This directory is maintained by the RFC Editor.  If you experience *
250-* any problems, please report them to rfc-editor@rfc-editor.org.    *
250-*                                     *
250-*=====*
250
TYPE A
200 Type okay.
PASV
227 Entering Passive Mode (128,9,176,20,249,176)
```

⇒ à ce stade, il faut vite se connecter à l'adresse et au port indiqué par la commande ci-dessous exécutée dans un autre terminal :

```
$ nc 128.9.176.20 63920 > rfc821.txt
```

⇒ il ne faut pas oublier de rediriger la sortie de **nc** dans le fichier de notre choix

```
RETR rfc821.txt
150 Data connection accepted from 139.124.187.4:48439; transfer starting for rfc821.txt (120432 bytes).
226 Transfer completed.
QUIT
221 Goodbye.
Connection closed by foreign host.
```

7 Le courrier électronique

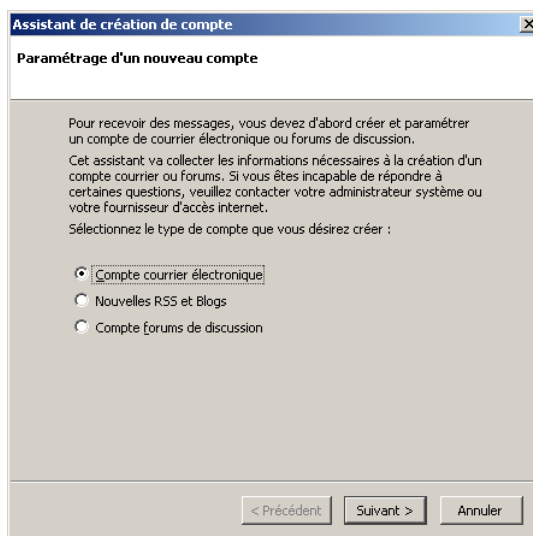
7.1 Clients de messagerie

Corrigé de l'exercice 22 (Utilisation de Thunderbird)

[\[Consulter l'énoncé\]](#)

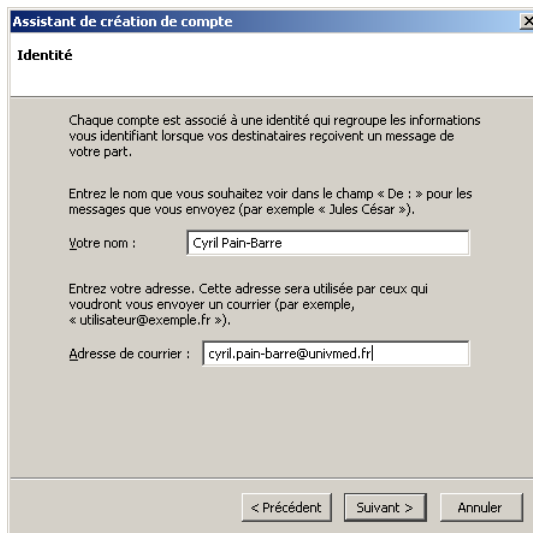
Après avoir demandé de ne pas importer les paramètres d'Outlook, le paramétrage de Thunderbird est guidé par un assistant. On suit les différentes étapes :

-



cliquer sur *Suivant*

-



après avoir indiqué son nom et son adresse email, cliquer sur *Suivant*

Assistant de création de compte

Information sur le serveur

Sélectionnez le type du serveur de réception.

POP IMAP

Entrez le nom du serveur de réception (par exemple, « pop.exemple.fr »).

Nom du serveur :

Décochez cette case pour stocker les messages de ce compte dans une arborescence indépendante. Ce compte sera ainsi considéré comme un compte de niveau supérieur. Dans le cas contraire, il fera partie du compte boîte globale stocké dans les dossiers locaux.

Utiliser la boîte globale (stocker les messages dans Dossiers locaux)

Entrez le nom du serveur d'envoi (SMTP) (par exemple, « smtp.exemple.fr »).

Nom du serveur :

< Précédent Suivant > Annuler

on indique le serveur POP3 (permettant de récupérer son courrier) et le serveur SMTP (permettant d'envoyer du courrier). Dans notre cas, il s'agit à chaque fois d'allegro. Puis cliquer sur *Suivant*

Assistant de création de compte

Nom d'utilisateur

Entrez le nom d'utilisateur entrant donné par votre fournisseur de courrier (par exemple, « martin »).

Nom d'utilisateur entrant :

Votre serveur sortant (SMTP), « allegro.iut.univ-aix.fr », est identique à votre serveur entrant. Votre nom d'utilisateur entrant sera utilisé pour la connexion à ce serveur. Il est possible de modifier les paramètres du serveur sortant en choisissant le menu Outils > Paramètres des comptes.

< Précédent Suivant > Annuler

ici on indique son nom d'utilisateur sur le serveur POP3. Pour vous, c'est *nnnppp*. Puis cliquer sur *Suivant*

Assistant de création de compte

Nom du compte

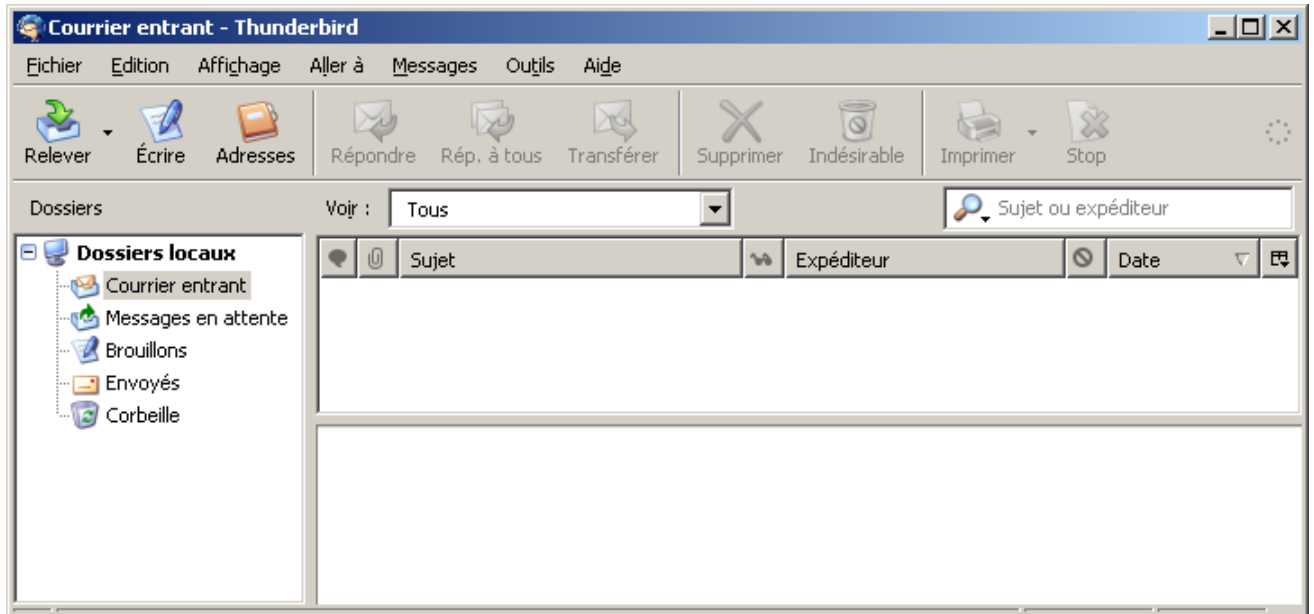
Entrez le nom avec lequel vous souhaitez vous référer à ce compte (par exemple « Compte Travail », « Compte personnel » ou « Compte Forums »).

Nom du compte :

< Précédent Suivant > Annuler

ici on donne un nom au compte que l'on vient de paramétrer, puisqu'on peut en avoir plusieurs. Puis cliquer sur *Suivant*

- Puis, après avoir validé les différents paramètres en cliquant sur *Terminer*, Thunderbird va télécharger le courrier présent sur le serveur POP. Pour cela, il vous demandera votre mot de passe sur ce serveur. Ensuite, l'interface de Thunderbird sera affichée :



- ◇ le bouton *Relever* permet de relever son courrier
- ◇ le bouton *Écrire* permet d'en envoyer

7.2 Format d'un message électronique

7.3 SMTP

7.3.1 Messages du protocole SMTP

7.3.2 Exercice

Corrigé de l'exercice 23 (Envoi du message anonyme)

[\[Consulter l'énoncé\]](#)

```
$ telnet allegro 25
Trying 139.124.187.4...
Connected to allegro.iut.univ-aix.fr (139.124.187.4).
Escape character is '^]'.
220 allegro.iut.univ-aix.fr ESMTPE postfix (2.2.5) (Mandriva Linux)
HELO mamachine.com
250 allegro.iut.univ-aix.fr
MAIL FROM:<tarzan@jungle.org>
250 Ok
RCPT TO:<cpb>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Tarzan of the Jungle <tarzan@jungle.org>
```

To: Cyril Pain-Barre <cpb@allegro>
Subject: Un message super interessant

**blablabla le message anonyme
et patati et patata**

.
250 Ok: queued as 37F92FC0

QUIT

221 Bye

Connection closed by foreign host.

Si on consulte ce message par mail, voici ça donne :

\$ **mail**

mailx version nail 11.25 7/29/05. Type ? for help.

"/var/spool/mail/cpb": 1 message 1 new

>N 1 Tarzan of the Jung Tue May 13 10:51 16/619 Un message super interessant
? 1

Message 1:

From tarzan@jungle.org Tue May 13 10:51:50 2008

Return-Path: <tarzan@jungle.org>

X-Original-To: cpb

Delivered-To: cpb@allegro.iut.univ-aix.fr

From: Tarzan of the Jungle <tarzan@jungle.org>

To: Cyril Pain-Barre <cpb@allegro.iut.univ-aix.fr>

Subject: Un message super interessant

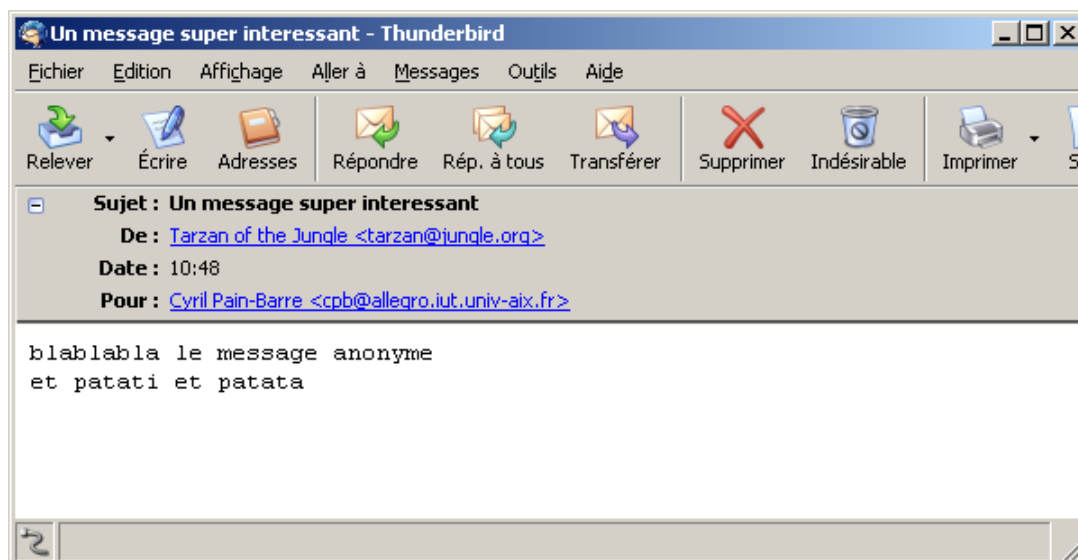
Date: Tue, 13 May 2008 10:48:53 +0200 (CEST)

Status: R

blablabla le message anonyme
et patati et patata

? **x**

Si on le récupère par Thunderbird et qu'on double-clique dessus, voici ce que l'on obtient :



7.4 Étude de la RFC de POP3

Corrigé de l'exercice 24 (récupération de messages avec POP3)

[\[Consulter l'énoncé\]](#)

Voici la trace de la discussion avec le serveur POP3 d'allegro, le reste ne nécessitant pas de corrigé :

```
$ telnet allegro 110
Trying 139.124.187.4...
Connected to allegro.iut.univ-aix.fr (139.124.187.4).
Escape character is '^]'.
+OK Qpopper (version 4.0.8) at allegro.iut.univ-aix.fr starting.
USER cpb
+OK Password required for cpb.
PASS mon-mot-de-passe
+OK cpb has 2 visible messages (0 hidden) in 1267 octets.
LIST
+OK 2 visible messages (1267 octets)
1 632
2 635
.
RETR 2
+OK 635 octets
Return-Path: <cpb@allegro.iut.univ-aix.fr>
X-Original-To: cpb
Delivered-To: cpb@allegro.iut.univ-aix.fr
Received: by allegro.iut.univ-aix.fr (Postfix, from userid 5778)
        id EED5AFC0; Tue, 13 May 2008 11:30:22 +0200 (CEST)
Date: Tue, 13 May 2008 11:30:22 +0200
From: cyril.pain-barre@univmed.fr
To: cpb@allegro.iut.univ-aix.fr
Subject: message 2
Message-ID: <48295fae.bLe5Hd8M/R82Mj9Q%cyril.pain-barre@univmed.fr>
User-Agent: nail 11.25 7/29/05
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-UIDL: ESp!!3$6!!NPD!!A%A"!

re blablabla le message 2
....
fin du message 2

.
DELE 2
+OK Message 2 has been deleted.
QUIT
+OK Pop server at allegro.iut.univ-aix.fr signing off.
Connection closed by foreign host.
```

8 Simulateur : Nat/Pat et firewall

Corrigé de l'exercice 12 (Simulation Nat/Pat et firewall)

[\[Consulter l'énoncé\]](#)

1. ... pas de corrigé pour cette question ...
2. L'activation du Nat/Pat ne devrait pas poser de problèmes.
Voici le [fichier xml](#) qui correspond à cette question.
3. La configuration des ports écoutés ne devrait pas poser de problèmes.
Voici le [fichier xml](#) qui correspond à cette question.
4. Les redirections demandées sont les suivantes :

- sur st1 :

N°	Type	Protocole	Ip privée	Port privé	Ip publique	Port public
01	mapping	UDP	192.168.2.2	69	172.11.0.3	69
02	mapping	TCP	192.168.0.3	22	172.11.0.3	22

- sur st5 :

N°	Type	Protocole	Ip privée	Port privé	Ip publique	Port public
01	mapping	TCP	192.168.1.8	21	172.12.0.4	21

- sur st9 :

N°	Type	Protocole	Ip privée	Port privé	Ip publique	Port public
01	mapping	TCP	192.168.6.12	80	172.12.0.3	80
02	mapping	TCP	192.168.5.13	22	172.12.0.3	22
03	mapping	TCP	192.168.6.14	21	172.12.0.3	21

Voici le [fichier xml](#) qui correspond à cette question.

5. Détaillons l'envoi d'une requête depuis la station st4 vers le serveur SSH de st13, ainsi que la réponse de st13 vers st4 :
 - envoi de la requête depuis st4 :

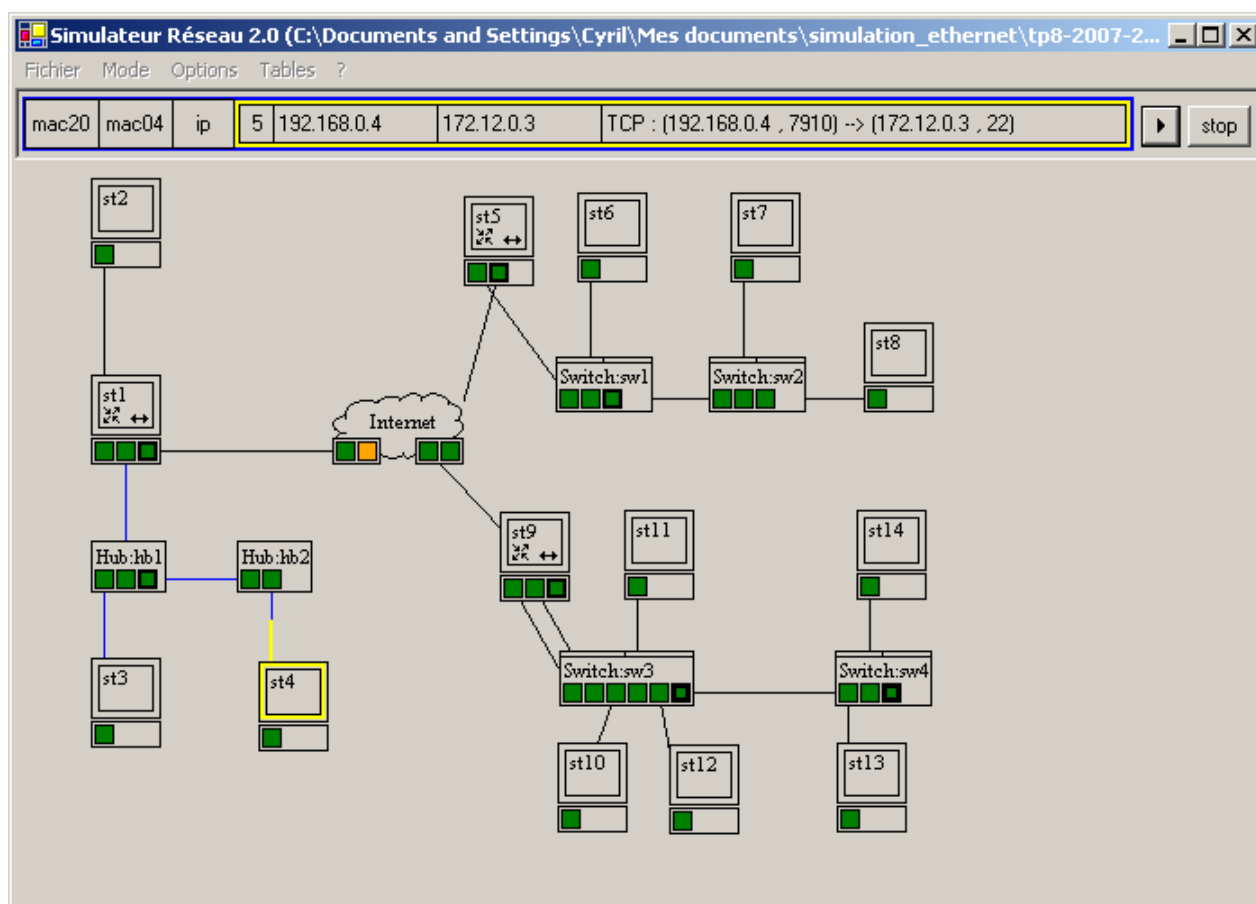
Paramétrage de l'envoi

Protocole :

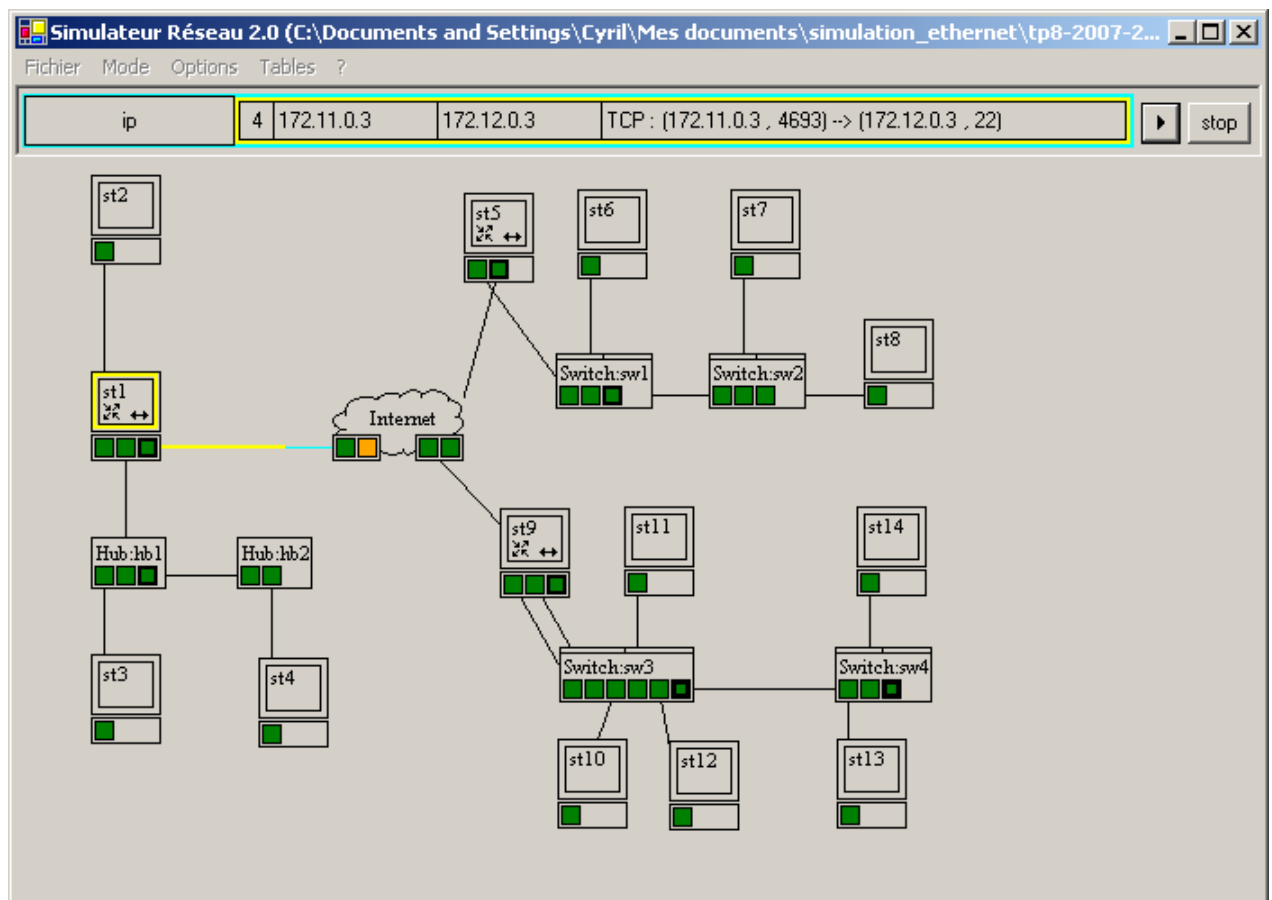
Adresse IP :

N° de port :

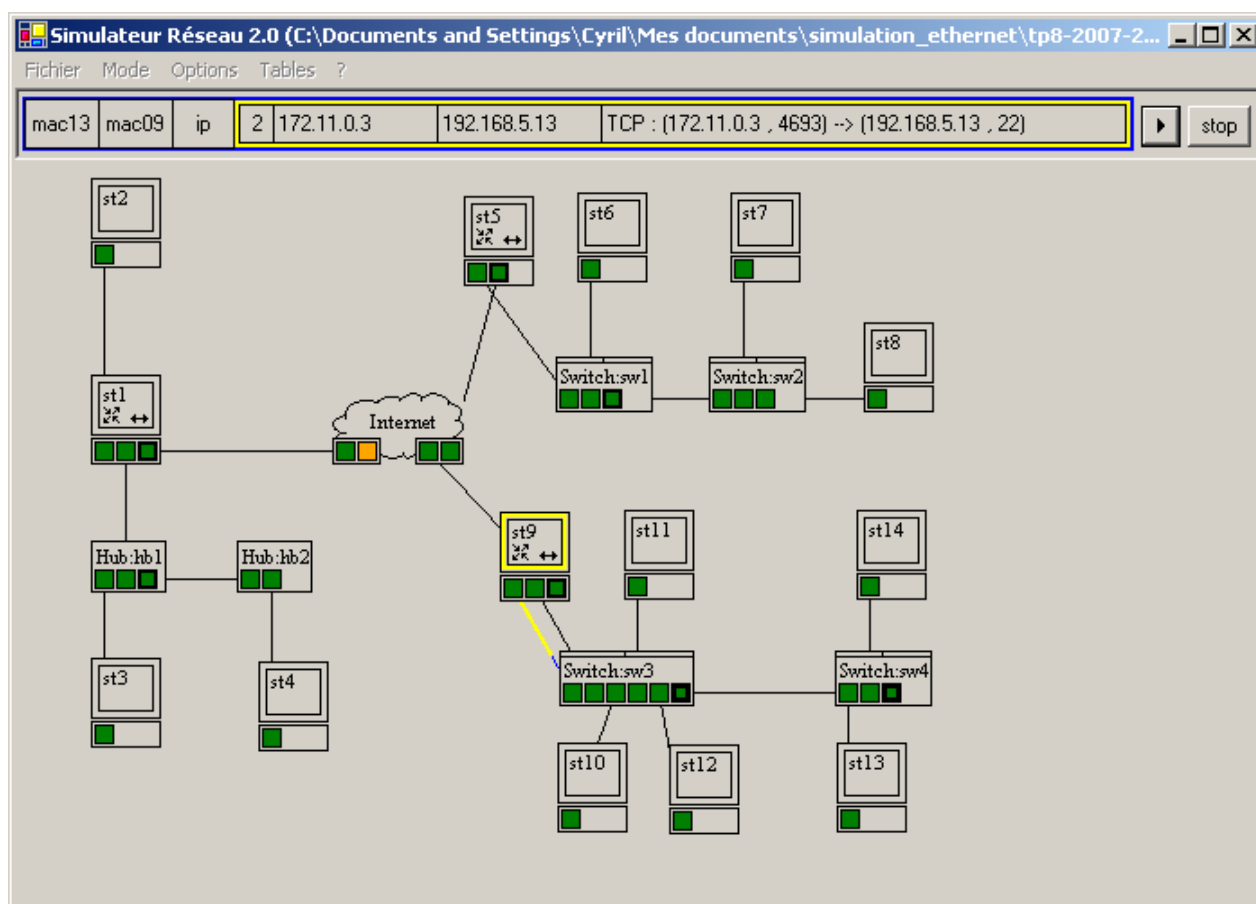
- vue du datagramme IP correspondant (sur le haut de la figure) en sortie de st4 :



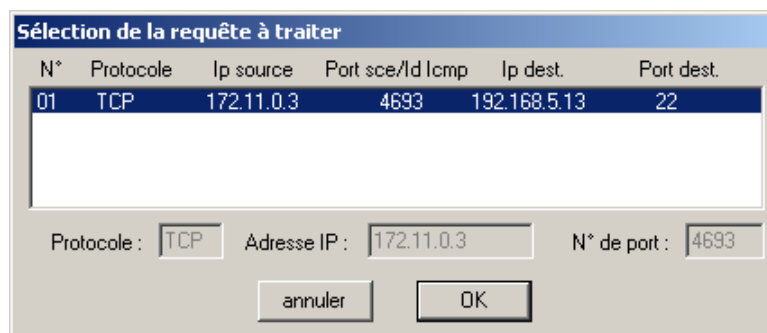
- effet du NATP réalisé par st1, où le datagramme IP a été modifié :



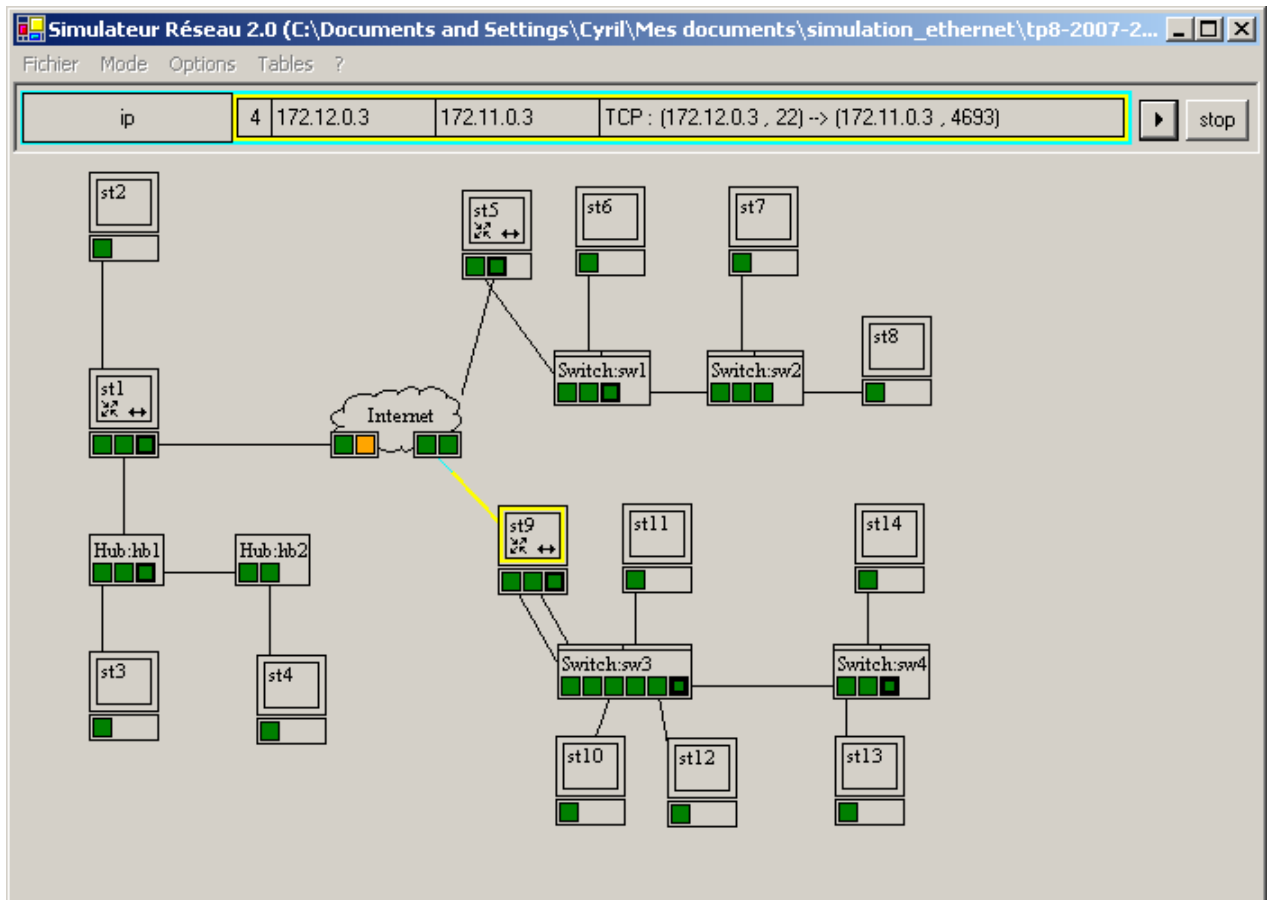
- effet du NATP réalisé par st9, où le datagramme IP a encore été modifié :



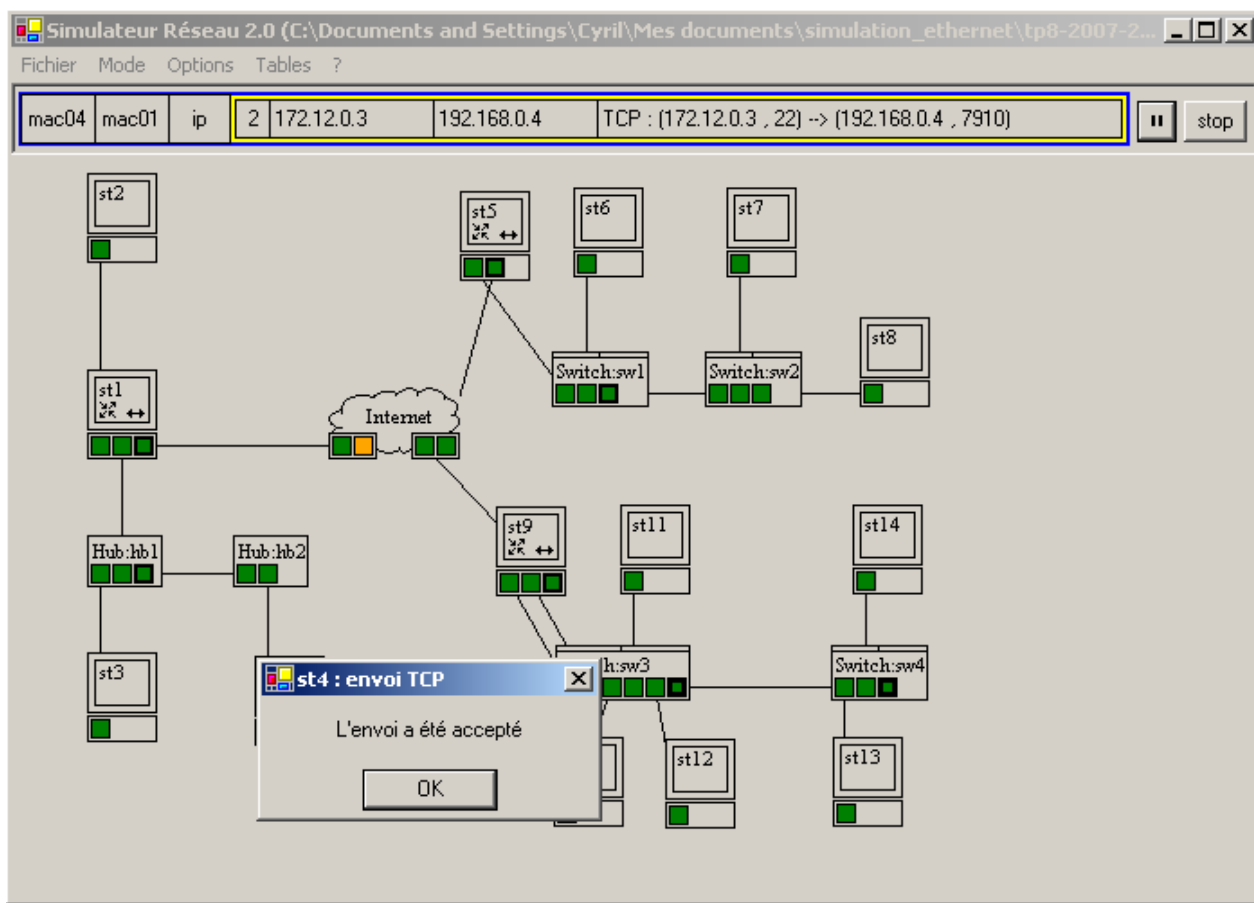
- envoi de la réponse depuis st13 :



- effet du NATP réalisé par st9 sur la réponse :



- effet du NAPT réalisé par st1 :



6. La table de filtrage sur st9 est :

N°	Entrée	Sortie	Prot.	Ip source/n	Pt sce	Ip dest/n	Pt dest	Action
01	mac24	mac23	TCP	*	*	192.168.6.12/32	80	Accepter
02	mac24	mac23	TCP	*	*	192.168.6.14/32	21	Accepter
03	mac24	mac09	TCP	172.11.0.3/32	*	192.168.5.13/32	22	Accepter
04	mac24	*	ICMP	*	*	*	*	Accepter
05	mac24	*	*	*	*	*	*	Bloquer
06	*	mac24	*	*	*	*	*	Accepter

Voici le [fichier xml](#) qui correspond à cette question.