



INSTITUT
FRANCOPHONE
INTERNATIONAL



VNU
ĐẠI HỌC QUỐC GIA HÀ NỘI
Vietnam National University, Hanoi

TRAVAIL DE GROUPE CONCEPTION ET ARCHITECTURES DES RESEAUX

Période : du 06 Novembre 2017 au 17 Décembre 2017

Rédigé par :

**BIAKOTA BOMBIA Herbert Cephass,
MEDOU Daniel Magloire,
MILORME Pierre Rubens,
SYLLA Aboubakar**

Etudiant en Master 1 des Systèmes Intelligents et
Multimédia, IFI.

Promotion 21

Enseignant :

M. Nguyen Hong QUANG

**Année académique
2017-2018**

TABLE DES MATIERES

LISTE DES TABLEAUX ET FIGURES.....	Erreur ! Signet non défini.
TABLE DES MATIERES.....	2
INTRODUCTION.....	3
I. INFORMATION SUR LES INTERFACES	4
1. Information sur la carte réseau	4
2. Liste des interfaces	5
II. Configuration de l'interface réseau wifi.....	6
III. Table de routage	6
IV. Les informations sur le nom de domaine de google.com	7
V. Affichage des routes	7
1. Table de routage	7
2. Liste des routes traversées par un paquet	7
VI. Serveur de nom des domaines	8
1. Domaine ifi.edu.vn	8
2. Domaine fpt.com.vn	8
VII. Configuration de l'interface wifi.....	9
VIII. OUTILS POUR LA CAPTURE DES TRAME	11
.....	17

INTRODUCTION

Dans le présent, il est question pour nous de réaliser le TP1 dans le cadre du cours de Conception et Architecture des Réseaux donc les objectifs sont entre autre de connaître et de savoir utiliser les commandes de base de Linux/Unix pour configurer et tester la connexion réseau, de savoir configurer un poste de travail en réseau sous Linux/Unix sans faire recours aux outils graphiques, de savoir analyser les protocoles de communication à l'aide des programmes pour la capture des trames, être capable de concevoir une petite application réseau.

I. INFORMATION SUR LES INTERFACES

Dans cette partie, il est question pour nous de présenter les différentes informations que contient l'interface réseau d'une machine sous Linux/Unix.

1. Information sur la carte réseau

```
biakota@groupe05:~$ lspci | grep -i ethernet
00:19.0 Ethernet controller: Intel Corporation Ethernet Connection I218-LM (rev 04)
biakota@groupe05:~$
```

Figure 1: Information sur la carte réseau

2. Liste des interfaces

```
biakota@groupe05:~$ ifconfig -a
enp0s25  Link encap:Ethernet  HWaddr 28:d2:44:df:1d:7f
        inet adr:172.16.5.3  Bcast:172.16.5.255  Masque:255.255.255.0
        UP BROADCAST MULTICAST  MTU:1500  Metric:1
        Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1000
        Octets reçus:0 (0.0 B) Octets transmis:0 (0.0 B)
        Interruption:20 Mémoire:f0600000-f0620000

enp0s20u1 Link encap:Ethernet  HWaddr da:8e:77:93:cb:9a
        inet adr:192.168.42.131  Bcast:192.168.42.255  Masque:255.255.255.0
        adr inet6: fe80::8ce7:4cc8:db0:31cd/64 Scope:Lien
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        Packets reçus:517 erreurs:0 :0 overruns:0 frame:0
        TX packets:628 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1000
        Octets reçus:196111 (196.1 KB) Octets transmis:172503 (172.5 KB)

lo       Link encap:Boucle locale
        inet adr:127.0.0.1  Masque:255.0.0.0
        adr inet6: ::1/128 Scope:Hôte
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        Packets reçus:8665776 erreurs:0 :0 overruns:0 frame:0
        TX packets:8665776 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1
        Octets reçus:904030167 (904.0 MB) Octets transmis:904030167 (904.0 MB)

wlp3s0   Link encap:Ethernet  HWaddr 28:b2:bd:a9:18:5c
        inet adr:10.227.79.228  Bcast:10.227.79.255  Masque:255.255.252.0
        adr inet6: fe80::d687:85fb:4969:8438/64 Scope:Lien
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        Packets reçus:201899 erreurs:0 :0 overruns:0 frame:0
        TX packets:188443 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1000
        Octets reçus:151404033 (151.4 MB) Octets transmis:28213363 (28.2 MB)
```

Figure 2: Liste des interfaces réseaux possibles d'une machine

De part cette capture faite, fort est de constater que notre machine dispose de quatre interface réseaux qui sont :

- enp0s25 : Contient les détails sur l'interface réseau filaire tels que l'adresse IP de la machine « 172.16.5.3 », son adresse broadCast « 172.16.5.255 », son masque « 255.255.255.0 »
- enp0s20u1 : Contient les détails sur la deuxième interface réseau filaire tels que l'adresse IP de la machine (inet) « 192.168.42.131 », son adresse broadCast (Bcast) « 192.168.42.255 », son masque « 255.255.255.0 »
- lo : Adresse de la machine locale (localhost) « 127.0.0.1 », le masque est « 255.0.0.0 ».
- wlp3s0 : Contient les détails de l'interface réseau sans fil (Wifi) tels que l'adresse IP de la machine (inet) « 10.227.79.228 », son adresse broadCast (Bcast) « 10.227.79.255 », son masque « 255.255.252.0 »

Cependant, l'attribution d'une adresse IP à une interface réseau (filaire et sans fil) se fait via les commandes suivantes :

- ifconfig : Permet de configurer l'interface réseau en mémoire de la manière temporelle (ifconfig <interface> <address ip> Par exemple : ifconfig enp0s25 172.16.5.3). Le masque de sous-réseau est déterminé automatiquement en fonction de la classe de l'adresse IP. Si l'adresse est différente on peut le spécifier avec l'option netmask : ifconfig eth0

172.16.5.3 netmask 255.255.255.0. Pour voir si la carte réseau est bien configurée, on peut utiliser la commande: “ ifconfig <interface>” ex : ifconfig enp0s25

II. Configuration de l’interface réseau wifi

La configuration de réseau wifi se fait de manière suivante :

- 1- ifconfig : Permet de configurer l’interface réseau en mémoire de la manière temporelle (ifconfig <interface> <address ip> Par exemple : ifconfig wlp3s0 192.168.43.41).
- 2- nous pouvons aussi utiliser la commande vi pour editer le fichier /etc/network/interfaces

```
root@groupe05:/home/biakota# vi /etc/network/interfaces
```

Figure 3: dfghjlmjhgf

```
auto wlp3s0
iface wlp3s0 inet static
wireless-key azerty1A
wireless-ssid bbch
address 192.168.43.41
netmask 255.255.255.0
```

Figure 4: fghjluytrfg

Wlp3s0 : nom de l’interface réseau

Wireless-key : mot de passe du réseau ss

Wireless-ssid : identifiant du réseau sans fil

Address 192.168.43.41

Netmask :255.255.255.0

III. Table de routage

La commande suivant « route -n » nous permet de connaître la table de routage de notre machine.

```
biakota@groupe05: ~
biakota@groupe05:~$ route -n
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
0.0.0.0          10.227.76.1     0.0.0.0          UG    600    0         0 wlp3s0
10.227.76.0      0.0.0.0         255.255.252.0    U     600    0         0 wlp3s0
169.254.0.0      0.0.0.0         255.255.0.0      U    1000    0         0 enp0s25
172.16.5.0       0.0.0.0         255.255.255.0    U     0       0         0 enp0s25
```

Figure 5: Table de routage

Nous observons que notre machine, pour n’importe qu’elle destination, doit prendre la passerelle qui a pour adresse: « 10.227.76.1 » connecté sur l’interface wlp3s0. Aussi, les paquets en

direction du réseau «10.227.76.0» passeront par la route par défaut ; ça veut dire les routes non prises en compte dans la table de routage.

IV. Les informations sur le nom de domaine de google.com

Pour obtenir les informations sur une machine, nous disposons de la commande «nslookup google.com »

```
biakota@groupe05:~$ nslookup google.com
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.24.206
```

Figure 6: Rendu de la commande nslookup

V. Affichage des routes

1. Table de routage

La table de routage de notre machine pour qu'elle soit connue, nous devons exécuter la commande « route -n ». Ci-dessous nous pouvons voir le résultat de cette commande.

```
biakota@groupe05:~$ route -n
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
0.0.0.0          10.227.76.1     0.0.0.0          UG        600    0         0 wlp3s0
10.227.76.0      0.0.0.0         255.255.252.0    U         600    0         0 wlp3s0
169.254.0.0      0.0.0.0         255.255.0.0      U        1000    0         0 enp0s25
172.16.5.0       0.0.0.0         255.255.255.0    U         0       0         0 enp0s25
```

Figure 7: route -n

2. Liste des routes traversées par un paquet

Pour afficher les différents routeurs que traverse un paquet, nous pouvons utiliser la commande « traceroute adresseIp_du_serveur_distant » exp : «\$ traceroute 112.137.140.41»

```
biakota@groupe05:~$ traceroute 112.137.140.41
traceroute to 112.137.140.41 (112.137.140.41), 30 hops max, 60 byte packets
 1  192.168.42.129 (192.168.42.129)  0.689 ms  0.927 ms  0.658 ms
 2  logout.lan (10.227.76.1)  7.688 ms  7.522 ms  7.578 ms
 3  * * *
 4  172.31.99.21 (172.31.99.21)  7.749 ms  118.70.0.12 (118.70.0.12)  7.673 ms  172.31.99.21 (172.31.99.21)  8.182 ms
 5  static.vnpt-hanoi.com.vn (123.25.27.97)  8.240 ms  static.vnpt-hanoi.com.vn (123.25.27.93)  9.833 ms  8.356 ms
 6  118.70.2.85 (118.70.2.85)  8.271 ms  static.vnpt.vn (123.29.5.85)  6.129 ms  static.vnpt.vn (123.29.1.189)  6.051 ms
 7  203.113.158.105 (203.113.158.105)  5.989 ms  static.vnpt.vn (113.171.5.197)  6.728 ms  *
 8  static.vnpt.vn (113.171.5.10)  5.954 ms  localhost (27.68.228.25)  8.633 ms  localhost (27.68.228.37)  13.201 ms
 9  localhost (27.68.228.37)  12.420 ms  12.488 ms  static.vnpt.vn (123.29.16.86)  7.788 ms
10  localhost (27.68.229.234)  5.971 ms  localhost (27.68.228.37)  13.239 ms  localhost (27.68.229.237)  12.169 ms
11  localhost (27.68.229.226)  8.568 ms  localhost (27.68.229.50)  6.272 ms  6.296 ms
12  localhost (27.68.229.237)  10.527 ms  localhost (27.68.229.233)  7.474 ms  6.336 ms
13  112.137.140.41 (112.137.140.41)  4.694 ms  localhost (27.68.229.50)  4.766 ms  5.509 ms
```

Figure 8: Trace route/Information sur les routes (Routeur bout en bout)

VI. Serveur de nom des domaines

1. Domaine ifi.edu.vn

```
biakota@groupe05:~$ dig NS nom ifi.edu.vn

; <<>> DiG 9.10.3-P4-Ubuntu <<>> NS nom ifi.edu.vn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 21734
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nom.                                IN      NS

;; AUTHORITY SECTION:
.                10800    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2017121301 1800 900 604800 86400

;; Query time: 1126 msec
;; SERVER: 172.16.5.3#53(172.16.5.3)
;; WHEN: Wed Dec 13 22:05:43 +07 2017
;; MSG SIZE rcvd: 107

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4647
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ifi.edu.vn.                IN      NS

;; Query time: 1056 msec
;; SERVER: 172.16.5.3#53(172.16.5.3)
;; WHEN: Wed Dec 13 22:05:44 +07 2017
;; MSG SIZE rcvd: 39
```

Figure 9: Information sur le serveur de ifi.edu.vn

2. Domaine fpt.com.vn

```
biakota@groupe05:~$ dig NS nom fpt.com.vn

; <<>> DiG 9.10.3-P4-Ubuntu <<>> NS nom fpt.com.vn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 34214
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nom.                                IN      NS

;; AUTHORITY SECTION:
.                10295    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2017121301 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 172.16.5.3#53(172.16.5.3)
;; WHEN: Wed Dec 13 22:14:08 +07 2017
;; MSG SIZE rcvd: 107

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32353
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fpt.com.vn.                IN      NS

;; Query time: 1831 msec
;; SERVER: 172.16.5.3#53(172.16.5.3)
;; WHEN: Wed Dec 13 22:14:10 +07 2017
;; MSG SIZE rcvd: 39
```

Figure 10: Information sur le serveur de fpt.com.vn

VII. Configuration de l'interface wifi

Pour configurer l'interface wifi, nous avons deux moyens à notre disposition. Nous pouvons le faire par commandes ou modifions le fichier suivant « /etc/network/interfaces ». Cette dernière procédure nous permet de configurer une interface wifi sous linux sans faire recours à des outils graphiques.

```
root@groupe05:/home/biakota# vi /etc/network/interfaces
```

Figure 11: Syntaxe modification de l'interface réseau

Expérimentation: Il nous faut ajouter les lignes suivantes:

```
auto interface_wifi ;
iface interface_wifi inet dhcp;
wireless-essid perso;
wireless_mode managed ;
wireless_key haukhailvini
Au fichier interfaces en respectant bien la syntaxe.
```

```
auto wlp3s0
iface wlp3s0 inet static
wireless-key azerty1A
wireless-essid bbch
address 192.168.43.41
netmask 255.255.255.0
~
```

Figure 12: Informations à ajouter dans le fichier interface

Après modification des configurations, il faut redémarrer le service en exécutant la commande « /etc/init.d/networking restart » afin que la machine puisse prendre en compte la nouvelle configuration.

Désactivez les 2 interfaces lo et eth0: ifconfig lo down ; cette commande nous permet de désactiver l'interface loopback.

```
biakota@groupe05:~$ sudo ifconfig lo down
biakota@groupe05:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
^C
--- localhost ping statistics ---
77 packets transmitted, 0 received, 100% packet loss, time 76007ms
```

Figure 13: Désactivation de l'interface réseau

ifconfig wlp3s0 down ; cette commande nous permet de désactiver l'interface wifi

```
biakota@groupe05:~$ sudo ifconfig wlp3s0 down
biakota@groupe05:~$
```

Figure 15: Désactivation de l'interface réseau wifi

```
biakota@groupe05:~$ ping 192.168.1.107
PING 192.168.1.107 (192.168.1.107) 56(84) bytes of data.
From 192.168.8.52 icmp_seq=1 Destination Host Unreachable
From 192.168.8.52 icmp_seq=2 Destination Host Unreachable
From 192.168.8.52 icmp_seq=3 Destination Host Unreachable
From 192.168.8.52 icmp_seq=4 Destination Host Unreachable
From 192.168.8.52 icmp_seq=5 Destination Host Unreachable
From 192.168.8.52 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.1.107 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 70
38ms
pipe 3
```

Figure 16: test de l'état de ping sur l'interface wifi

```
biakota@groupe05:~$ iwconfig
wlp3s0 IEEE 802.11bgn ESSID:"Ktx My Dinh"
Mode:Managed Frequency:2.462 GHz Access Point: AC:86:74:49:
CA:B2
Bit Rate=144.4 Mb/s Tx-Power=22 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
Link Quality=47/70 Signal level=-63 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:30 Missed beacon:0

lo no wireless extensions.

enp0s25 no wireless extensions.
```

Figure 17: test de l'état de ping sur l'interface wifi

VIII. OUTILS POUR LA CAPTURE DES TRAME

2.1 Analyse du protocole ARP

Le protocole ARP (Address Resolution Protocol) est un protocole qui permet de retrouver les machines (adresse MAC) à partir des adresses IP. Pour ce fait il est nécessaire qu'une machine connectée puisse connaître l'adresse des autres machines, précisément l'adresse MAC de la carte réseau utilisée pour la communication. En d'autre terme, ce niveau que le protocole ARP intervient pour permettre aux machines de retrouver l'adresse MAC à partir d'un adresse IP.

Au niveau de chaque machine, dispose d'une cache ARP contenant les adresses déjà résolues qu'elle examine dans un premier temps pour faire la résolution. Au cas où cette adresse ne figure pas dans la cache, la machine envoie un paquet « ARP Request» en broadcast. Toute les machines connectées reçoivent le message mais seule la machine concernée répondra directement en unicast à la machine émettrice en émettant un paquet « ARP Reply» qui contient son adresse IP et MAC.

Description de la commande: La commande ARP permet de visualiser ou modifier la table du cache ARP de l'interface. Cette table peut être statique et (ou) dynamique. Elle donne la correspondance entre une adresse IP et une adresse MAC (Ethernet). A chaque nouvelle requête, le cache ARP de l'interface est mis à jour. Il y a un nouvel enregistrement. Cet enregistrement à une durée de vie (ttl ou Time To Live).

Voici un exemple de cache ARP obtenu avec la commande arp -va :

```
biakota@groupe05:~$ arp -va
logout.lan (10.227.76.1) à ac:86:74:49:ca:b2 [ether] sur wlp3s0
Entrées: 1      Ignorées: 0      Trouvées: 1
```

Figure 18: test avec arp

à l'issu de ce test nous remarquons que l'adresse IP et l'adresse MAC correspondante. Il n'y a qu'une entrée dans la table. Voici les principales options de la commande arp : arp -s (ajouter une entrée statique), exemple : arp -s 10.227.76.1 ac:86:74:49:ca:b2 arp -d (supprimer une entrée), exemple : arp -d 10.227.76.1 La commande netstat : dans ce travail nous avons utilisé de la commande netstat, qui permet de tester la configuration du réseau, visualiser l'état des connexions, établir des statistiques, notamment pour surveiller les serveurs. L'utilitaire mtr permet de voir le chemin suivi par paquet entre deux hots. Il combine parfaitement les principes de « ping » et « traceroute » dans ce sens qu'il permet d'avoir à intervalle de 1s l'état réel d'une route. Pour faire les vérifications, nous avons lancé la commande « mtr www.vnpt.com.vn ». Voici le résultat

```

biakota@groupe05: ~
My traceroute [v0.86]
groupe05.tp1.ifi (0.0.0.0) Sun Dec 3 00:40:41 2017
Keys: Help Display mode Restart statistics Order of fields quit
          Packets          Pings
Host      Loss%  Snt   Last   Avg   Best  Wrst StDev
1.  logout.lan      0.0%  18     2.7    3.7    1.6  22.2   5.1
2.  ???
3.  172.31.99.21     0.0%  18     4.0   13.4    2.6 104.1  23.8
4.  static.vnpt-hanoi.com.vn 0.0%  18     6.3    6.8    2.8  29.0   5.8
5.  static.vnpt.vn   0.0%  18     5.2    7.7    3.1  16.2   4.1
6.  static.vnpt.vn   0.0%  18    12.7   20.6   12.7  72.1  15.1
7.  static.vnpt.vn   0.0%  18    15.6   16.4   12.3  43.8   7.1
8.  static.vnpt.vn   0.0%  18    13.3   15.1   12.4  22.4   2.9
9.  10310.sgw.equinix.com 0.0%  18    36.8   38.1   35.0  49.0   3.3
10. ae-8.pat2.sgx.yahoo.com 0.0%  17    35.9   39.2   35.9  44.7   3.0
11. et-3-1-0.pat2.twi.yahoo.com 0.0%  17    91.9   91.9   88.9  97.1   2.8
12. ae-34.msr2.tw1.yahoo.com 0.0%  17    96.2   92.2   88.5 108.5   4.6
13. po-254.bas2-2-prd.tw1.yahoo.com 0.0%  17   112.1   93.1   89.6 112.1   5.9
14. w2.src.vip.tw1.yahoo.com 0.0%  17    93.4   91.3   89.6  96.2   1.4

```

Figure 18: affichage de mtr

la commande Mtr permettant ainsi de donner des résultats plus complets et mis à jour en temps réel (toutes les secondes par défaut) sur l'état d'une route. MTR utilise les paquets ICMP pour tester l'affirmation et la circulation entre deux points sur l'internet. En démarre mtr avec la commande `mtr www.vnpt.com.vn` Constat :

- mtr envoie une séquence de requête ICMP à chacun pour déterminer la qualité de la liaison à chaque machine. Il affiche les statistiques courantes de chaque machine.
- On peut aller à VNPT directement. Static.vdc.vn est l'adresse de VNPT et 10.10.10.2 est un réseau privé de VNPT
- Lost: Le pourcentage des paquets perdus.
- Snt : Le nombre de paquet envoyés avec succès.
- Last : La latence du dernier paquet envoyé.
- Avg : Le temps moyenne pour envoyer un paque
- Best : Le meilleur temps qu'un paquet mis lors de son envoi
- Wrst : Le pire temps pour envoyer un paquet StDev (Standard Déviation):

Le standard de la Dissidence

```

blakota@groupe05:~$ traceroute www.vnpt.com.vn
traceroute to www.vnpt.com.vn (123.31.27.130), 30 hops max, 60 byte packets
 1  logout.lan (10.227.76.1)  3.552 ms  6.707 ms  9.735 ms
 2  * * *
 3  118.70.0.12 (118.70.0.12)  25.376 ms  172.31.99.21 (172.31.99.21)  17.751 ms
 4  static.vnpt-hanoi.com.vn (123.25.27.97)  25.735 ms  *  113.22.4.117 (113.22.4.117)  25.722 ms
 5  static.vnpt.vn (113.171.21.237)  25.719 ms  118.70.2.85 (118.70.2.85)  25.704 ms
 6  118.70.2.89 (118.70.2.89)  26.183 ms  static.vnpt.vn (113.171.33.42)  10.250 ms
 7  static.vnpt.vn (113.171.5.9)  11.907 ms  *  11.906 ms
 8  *  static.vnpt.vn (113.171.5.9)  12.063 ms  localhost (123.31.27.130)  12.060 ms

```

Figure 18: test avec traceroute

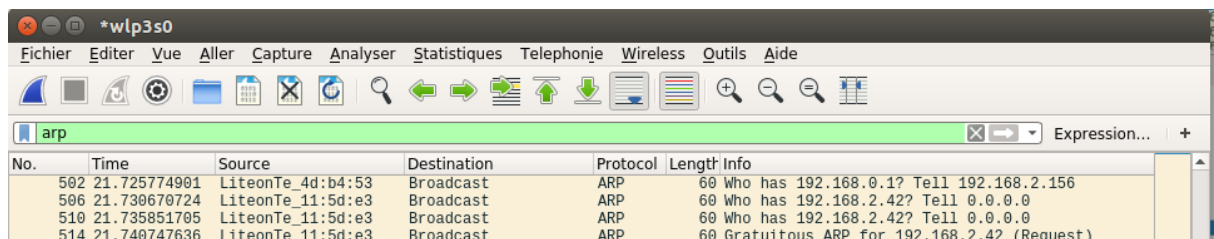
2.1. Analyse du protocole arp

8 chemins d'adresse 1 dont un chemin est masqué.

Analyse des Paquets avec Wireshark:

Wireshark est un analyseur de paquets libre utilisé dans le dépannage et l'analyse de réseaux informatiques

En effectuant la commande ping 172.16.5.255, et nous voyons que la requête est envoyée en broadcast, et l'hôte avec l'adresse 172.16.5.3 (machine émettrice)



No.	Time	Source	Destination	Protocol	Length	Info
502	21.725774901	LiteonTe_4d:b4:53	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.2.156
506	21.730670724	LiteonTe_11:5d:e3	Broadcast	ARP	60	Who has 192.168.2.42? Tell 0.0.0.0
510	21.735851705	LiteonTe_11:5d:e3	Broadcast	ARP	60	Who has 192.168.2.42? Tell 0.0.0.0
514	21.740747636	LiteonTe_11:5d:e3	Broadcast	ARP	60	Gratuitous ARP for 192.168.2.42 (Request)

Figure 19: test avec arp

2.2. Analyse du protocole ICMP

ping sur google (216.58.197.110)

No.	Time	Source	Destination	Protocol	Length	Info
134	10.075537388	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=18/4608, t...
135	10.130055503	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=18/4608, t...
144	11.077210027	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=19/4864, t...
145	11.131479243	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=19/4864, t...
153	12.078701057	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=20/5120, t...
162	12.132593993	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=20/5120, t...
172	13.079738587	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=21/5376, t...
183	13.133694343	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=21/5376, t...
190	14.080818806	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=22/5632, t...
200	14.152504502	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=22/5632, t...
213	15.082570851	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=23/5888, t...
214	15.136986829	216.58.197.110	192.168.8.52	ICMP	98	Echo (ping) reply id=0x37ba, seq=23/5888, t...
227	16.084125359	192.168.8.52	216.58.197.110	ICMP	98	Echo (ping) request id=0x37ba, seq=24/6144, t...

Figure 20: test avec traceroute

Afin de pouvoir capturer les trames nous allons utiliser la commande suivante : 'tcpdump',

D'abord il faut lancer la commande mentionnée ci-dessous afin d'attendre la requête (télécharger le fichier)

Fichier : `sudo tcpdump -i wlp3s0 port http`

```
biakota@groupe05:~$ sudo tcpdump -i wlp3s0 port http
[sudo] Mot de passe de biakota :
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Figure 21: test avec arp

2.3. Analyse du protocole TCP

Deuxièmement, il faut lancer le téléchargement:

- La commande pour capturer des trames avec 'tcpdump' en

téléchargeant un fichier à partir de la commande

`wget http://fad.ifi.edu.vn/ififad/file.php/28/documents/WS_user-guide-a4.pdf`

`sudo tcpdump -w « nom de fichier`

```

biakota@groupe05:~$ wget http://fad.ifi.edu.vn/itifad/file.php/28/documents/WS_u
ser-guide-a4.pdf
--2017-12-18 04:30:11-- http://fad.ifi.edu.vn/itifad/file.php/28/documents/WS_u
ser-guide-a4.pdf
Résolution de fad.ifi.edu.vn (fad.ifi.edu.vn)... 112.137.140.42
Connexion à fad.ifi.edu.vn (fad.ifi.edu.vn)|112.137.140.42|:80... connecté.
requête HTTP transmise, en attente de la réponse... 303 See Other
Emplacement : http://fad.ifi.edu.vn/itifad/login/index.php [suivant]
--2017-12-18 04:30:11-- http://fad.ifi.edu.vn/itifad/login/index.php
Réutilisation de la connexion existante à fad.ifi.edu.vn:80.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [text/html]
Enregistre : «WS_user-guide-a4.pdf.2»

WS_user-guide-a4.pdf      [ <=>          ] 10,10K  --.-KB/s   in 0,01s
2017-12-18 04:30:12 (1,03 MB/s) - «WS_user-guide-a4.pdf.2» enregistré [10344]

```

Capture en cours de wlp3s0

Fichier Éditer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
71	5.983103434	192.168.8.52	112.137.140.42	TCP	74	36624 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK...
72	5.986828309	112.137.140.42	192.168.8.52	TCP	74	80 → 36624 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS...
73	5.986893992	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=8...
74	5.987043511	192.168.8.52	112.137.140.42	HTTP	256	GET /itifad/file.php/28/documents/WS_user-guide-a4.p...
75	5.993668669	112.137.140.42	192.168.8.52	TCP	66	80 → 36624 [ACK] Seq=1 Ack=191 Win=6912 Len=0 TSval=...
85	6.656459423	112.137.140.42	192.168.8.52	HTTP	822	HTTP/1.1 303 See Other (text/html)
86	6.656497144	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=191 Ack=757 Win=30720 Len=0 TSv...
87	6.656524693	112.137.140.42	192.168.8.52	HTTP	822	[TCP Spurious Retransmission] HTTP/1.1 303 See Other...
88	6.656537198	192.168.8.52	112.137.140.42	TCP	78	[TCP Dup ACK 86#1] 36624 → 80 [ACK] Seq=191 Ack=757...
89	6.656754736	192.168.8.52	112.137.140.42	HTTP	309	GET /itifad/login/index.php HTTP/1.1
90	6.665027028	112.137.140.42	192.168.8.52	TCP	66	80 → 36624 [ACK] Seq=757 Ack=434 Win=7936 Len=0 TSva...
92	6.961037237	112.137.140.42	192.168.8.52	TCP	2922	[TCP segment of a reassembled PDU]
93	6.961084493	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=434 Ack=3613 Win=36480 Len=0 TS...
94	6.966034445	112.137.140.42	192.168.8.52	TCP	4350	[TCP segment of a reassembled PDU]
95	6.966066321	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=434 Ack=7897 Win=45056 Len=0 TS...
96	6.971040997	112.137.140.42	192.168.8.52	HTTP	3905	HTTP/1.1 200 OK (text/html)
97	6.971070612	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=434 Ack=11736 Win=52736 Len=0 T...
98	6.971783761	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [FIN, ACK] Seq=434 Ack=11736 Win=52736 Le...
99	6.974980250	112.137.140.42	192.168.8.52	TCP	66	80 → 36624 [FIN, ACK] Seq=11736 Ack=435 Win=7936 Len...
100	6.975099999	192.168.8.52	112.137.140.42	TCP	66	36624 → 80 [ACK] Seq=435 Ack=11737 Win=52736 Len=0 T...

Frame 97: 66 bytes on wire (528 bits) - 66 bytes captured (528 bits) on interface 0

- Ethernet II, Src: IntelCor_a9:18:5c (28:b2:b0:a9:18:5c), Dst: Routerbo_01:91:b0 (64:d1:54:01:91:b0)
- Internet Protocol Version 4, Src: 192.168.8.52, Dst: 112.137.140.42
- Transmission Control Protocol, Src Port: 36624, Dst Port: 80, Seq: 434, Ack: 11736, Len: 0

0000 64 d1 54 01 91 b0 28 b2 bd a9 18 5c 08 00 45 00 d.T...(.E.

0010 00 34 5f 8c 40 00 40 06 15 a8 c0 a8 08 34 70 89 .4..0.0.4p.

0020 8c 2a 8f 10 00 50 18 90 c1 0a 56 04 8c f1 80 10 *. .P. . .V.....

0030 01 9c 3f 3a 00 00 01 01 08 0a 00 0c e1 d3 17 37 .7:.....7

0040 2b 4f

Nous pouvons constater qu'à la fin de la phase de transaction, le serveur s'est déconnecté. Nous allons mentionner cette phase dans les figures ci-dessous ;

Le diagramme ci-dessous illustre les échanges entre le client (notre machine) et le serveur lorsque le protocole TCP est utilisé.

2.4 Analyse du protocole Telnet

Nous allons utiliser 2 machines :

- L'adresse du client telnet : 172.16.5.4

- L'adresse du serveur telnet : 172.16.5.3

Côté du serveur et client : Tous utilisent le port 23 pour entendre et envoient les requêtes. Et ouvrent un port quelconque (sur l'image ci-dessus, c'est le port 41092) pour entendre la réponse du server.

telnet					
No.	Time	Source	Destination	Protocol	Length Info
19	26.062230220	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
20	26.062589428	172.16.5.3	172.16.5.4	TELNET	55 Telnet Data ...
22	26.288256237	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
23	26.288571891	172.16.5.3	172.16.5.4	TELNET	55 Telnet Data ...
25	27.571797038	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
26	27.572160045	172.16.5.3	172.16.5.4	TELNET	58 Telnet Data ...
28	27.709132840	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
29	27.709446863	172.16.5.3	172.16.5.4	TELNET	58 Telnet Data ...
31	27.848210667	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
32	27.848390441	172.16.5.3	172.16.5.4	TELNET	55 Telnet Data ...
34	29.708936202	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
35	29.709176854	172.16.5.3	172.16.5.4	TELNET	55 Telnet Data ...
37	29.812254177	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
38	29.812477013	172.16.5.3	172.16.5.4	TELNET	55 Telnet Data ...
42	30.820333542	172.16.5.4	172.16.5.3	TELNET	60 Telnet Data ...
43	30.820492035	172.16.5.3	172.16.5.4	TELNET	56 Telnet Data ...
45	30.860746135	172.16.5.3	172.16.5.4	TELNET	886 Telnet Data ...

▶ Frame 19: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: Inventec_31:6d:61 (00:8c:fa:31:6d:61), Dst: LcfcHefe_df:1d:7f (28:d2:44:df:1d:7f)

▶ Internet Protocol Version 4, Src: 172.16.5.4, Dst: 172.16.5.3

▶ Transmission Control Protocol, Src Port: 1299, Dst Port: 23, Seq: 1, Ack: 1, Len: 1

▶ Telnet

0000	28 d2 44 df 1d 7f 00 8c fa 31 6d 61 00 00 45 00	(.D.....1ma..E.
0010	00 29 26 dd 40 00 00 06 71 ca ac 10 05 04 ac 10)&. ... q.....
0020	05 03 05 13 00 17 f7 39 c1 08 ab ef b1 e9 50 189.....P.
0030	08 03 de 5a 00 00 4c 00 00 00 00 00	...Z..L.....

CONCLUSION

de tout ce qui précède, Ce présent TP le travail effectué nous a permis d'analyser des différents commandes de Configuration d'une station de réseau sous linux, ce travail nous a permis de maîtriser les configurations de base d'un réseau sous linux et l'administration d'un réseau celui-ci. s et découvrir de de nouveaux certain valeur ajoutée telle que : **wget**, **altitude**, **mtr**,

nslookup, Le protocole TCP (Transmission Control Protocol, Protocole de contrôle de la transmission), Le protocole ARP.