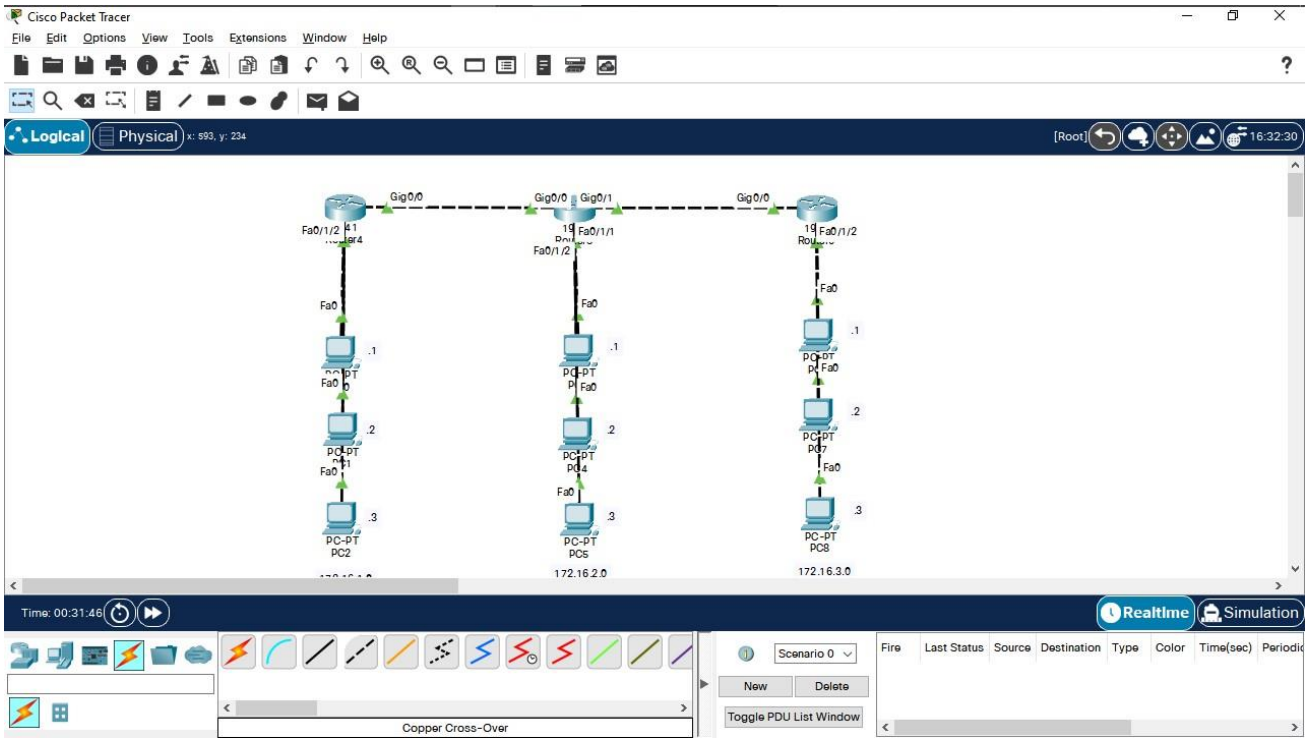
TPRESEAUUNIX

**- TP exercices linux Configuration IP - Cryptage des transmissions - Exploitation de la trame**

## Exercice 1 : Configuration IP

1) Effectuez le câblage du réseau selon la maquette de la figure




1. Indiquez pour chaque segment le type de câble nécessaire (droit ou croisé).
   - Le type de câble nécessaire est le câble croisé

2) Utilisez la commande ifconfig pour configurer votre adresse IP et le masque de sous-réseau.

```
┌──(bamba㉿kali)-[~]
└─$ sudo ifconfig eth0 172.16.1.1/24

┌──(bamba㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.1  netmask 255.255.255.0  broadcast 172.16.1.255
        ether 00:0c:29:38:ae:dc  txqueuelen 1000  (Ethernet)
        RX packets 336  bytes 51041 (49.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 591  bytes 59034 (57.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3) Utilisez la commande route pour configurer votre passerelle de sortie.

```
┌──(bamba㉿kali)-[~]
└─$ route -N
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
172.16.1.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0

┌──(bamba㉿kali)-[~]
└─$ sudo route add default gw 172.16.1.254

┌──(bamba㉿kali)-[~]
└─$ route -N
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         172.16.1.254    0.0.0.0         UG    0      0        0 eth0
172.16.1.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

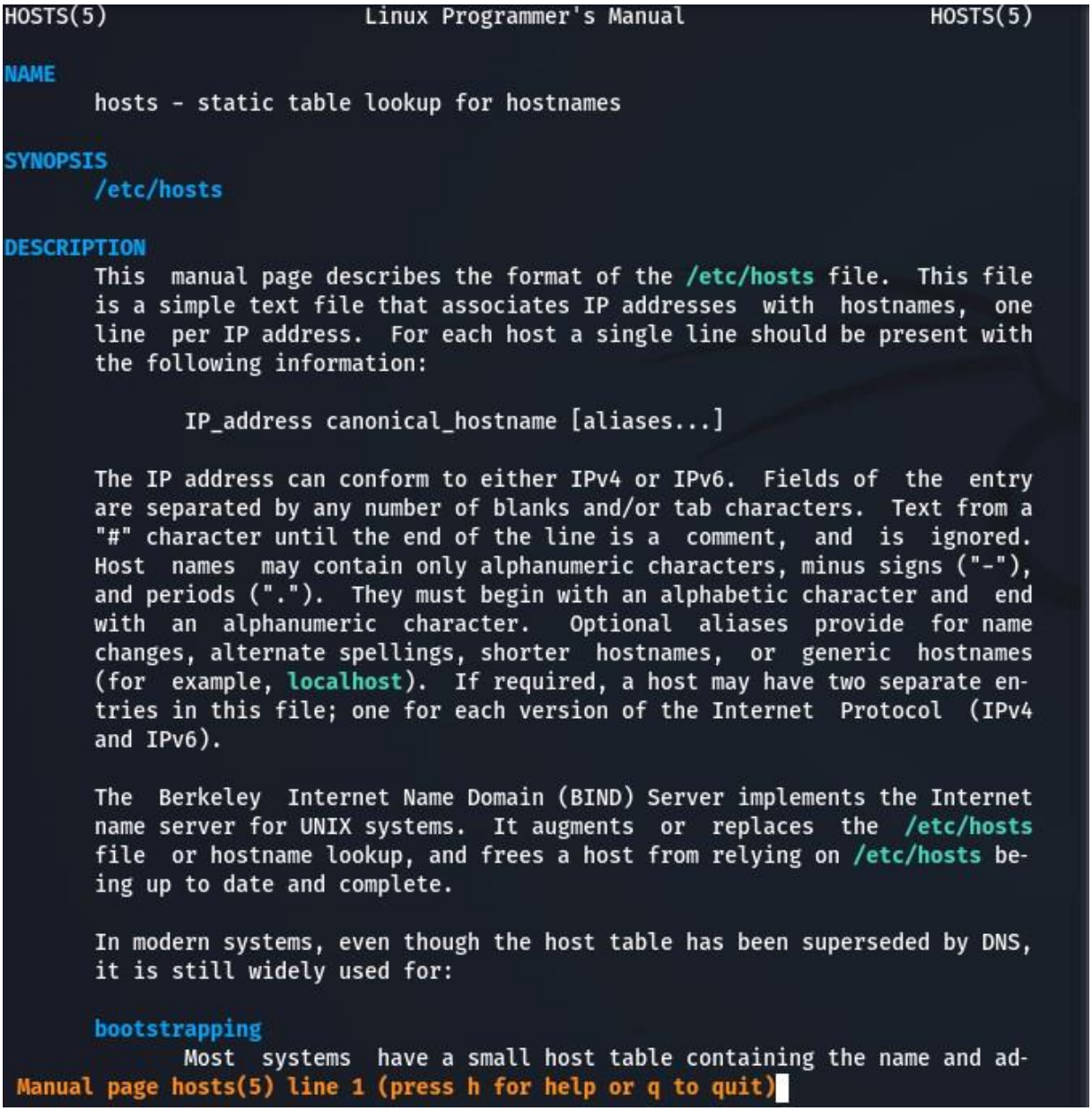
**Exercice 2: Le fichier *`/etc/hosts`***

1) Utilisez la commande ping pour joindre les autres machines. Peut-on utiliser le nom des machines a la place de l'adresse IP?

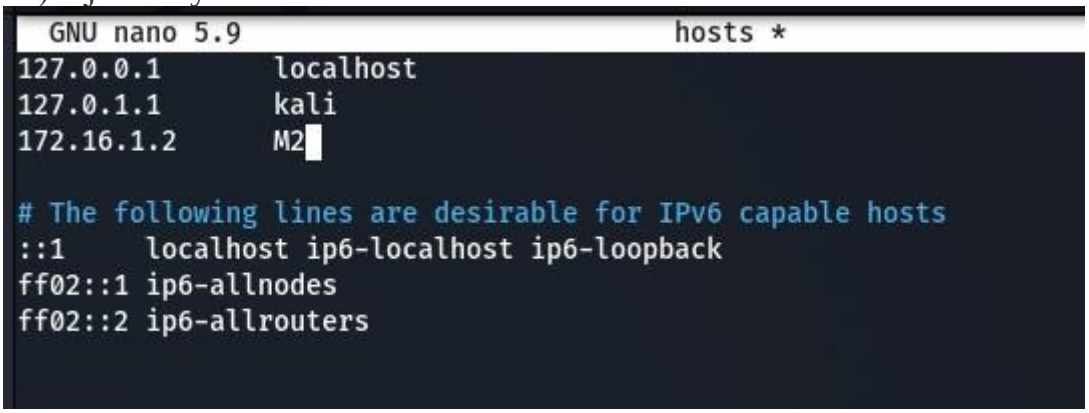
```
┌──(bamba㉿kali)-[~]
└─$ ping -c4 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=0.457 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=0.705 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=64 time=2.26 ms
64 bytes from 172.16.1.2: icmp_seq=4 ttl=64 time=0.714 ms

--- 172.16.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.457/1.033/2.257/0.714 ms
```

Nous ne pouvons pas utiliser le nom des machines a la place de l'adresse cas ils n'ont pas été définie

2) Utilisez le man pour trouver des informations sur le fichier /etc/hosts.




3°) Ajoutez-y les noms des autres machines.



4) Que peut-on dire maintenant pour la question 1?

```
┌──(bamba㉿kali)-[~]
└─$ ping -c4 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=0.447 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=0.663 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=64 time=0.818 ms
64 bytes from 172.16.1.2: icmp_seq=4 ttl=64 time=0.643 ms

--- 172.16.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 0.447/0.642/0.818/0.131 ms

┌──(bamba㉿kali)-[~]
└─$ ping -c4 M2
PING M2 (172.16.1.2) 56(84) bytes of data.
64 bytes from M2 (172.16.1.2): icmp_seq=1 ttl=64 time=0.502 ms
64 bytes from M2 (172.16.1.2): icmp_seq=2 ttl=64 time=0.631 ms
64 bytes from M2 (172.16.1.2): icmp_seq=3 ttl=64 time=0.696 ms
64 bytes from M2 (172.16.1.2): icmp_seq=4 ttl=64 time=0.782 ms

--- M2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 0.502/0.652/0.782/0.102 ms
```

**Exercice 3 : Connexion a une autre machine**

1) Il existe plusieurs commandes permettant de se connecter et d'utiliser a distance une
machine. Utilisez et indiquez les différences entre les commandes telnet et ssh.

```
all@ubuntu:~$ ssh bamba@172.16.1.1
bamba@172.16.1.1's password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun  6 21:35:05 2022 from 192.168.0.3
┌──(bamba㉿kali)-[~]
└─$
```

SSH et Telnet sont deux protocoles réseau qui permettent aux utilisateurs de se connecter à des systèmes distants et d'exécuter des commandes sur ceux-ci.

L’accès à la ligne de commande d’un hôte distant est similaire dans les deux protocoles, mais la différence principale de ces protocoles dépend de la mesure de sécurité de chacun. SSH est hautement sécurisé que Telnet.

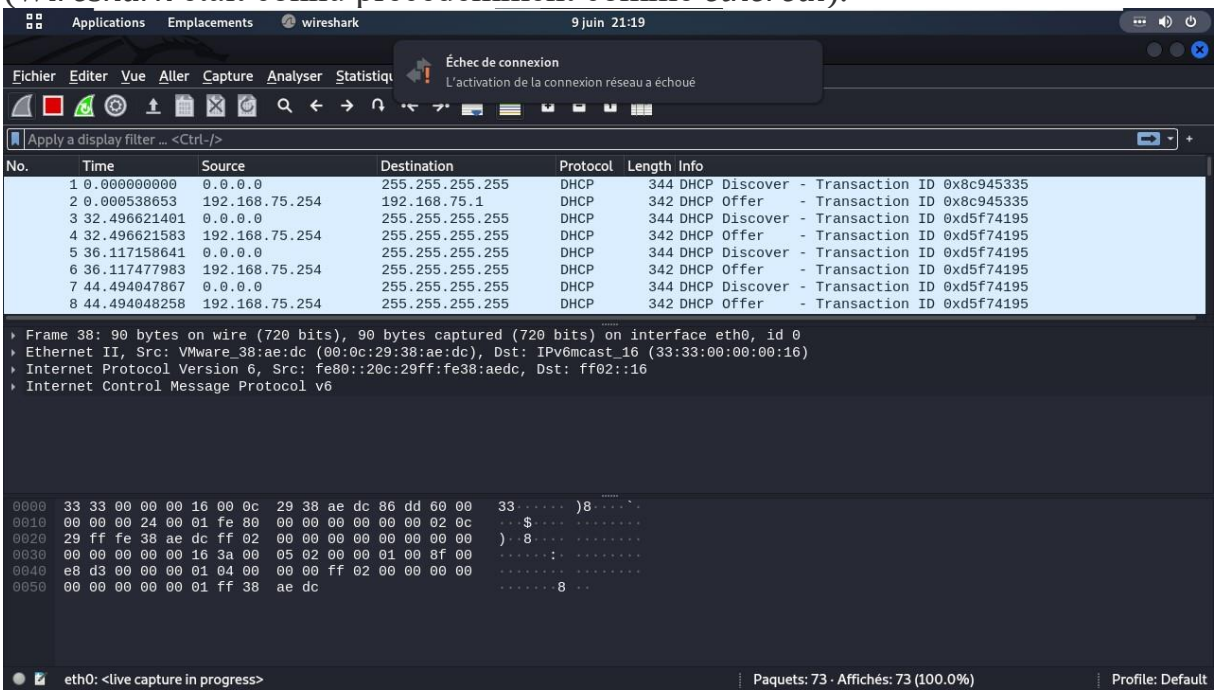
Par défaut, SSH utilise le port 22 et Telnet utilise le port 23 pour les communications, et les deux utilisent le standard TCP.

SSH envoie toutes les données dans un format crypté, mais Telnet envoie les données en texte brut. Par conséquent, SSH utilise un canal sécurisé pour transférer des données sur le réseau, mais Telnet utilise une manière normale de se connecter au réseau et de communiquer.

De plus, SSH utilise le cryptage à clé publique pour authentifier les utilisateurs distants, mais Telnet n’utilise aucun mécanisme d’authentification.

## Exercice 4 : Installation et prise en main de Wireshark

1) Après avoir configuré votre adresse IP pour pouvoir joindre toutes les machines de la
salle, installer le logiciel *wireshark* en utilisant la commande *apt-get install wireshark*.
(*Wireshark* était connu précédemment comme *ethereal*).




## Exercice 5: Récupération de mot de passe

1) Grace a une capture de trame depuis votre machine M1, récupérez le mot de passe d’un utilisateur d’une machine M2 effectuant une connexion ftp ou telnet sur une machine
M3.

**Exercice 6 : Exploitation de la trame**

1) Essayez d'exploiter le mieux possible la capture contenant ce mot de passe. Pour cela, réaliser, par exemple, un chronogramme.

2) Indiquez tous les problèmes que vous pouvez détecter dans cette capture (perte de trame, padding ethernet, réémission, double acquittement, etc.…). Vous pouvez également compléter cette capture par une autre capture montrant d'autres problèmes.

**Exercice 7 : Cryptage des transmissions**

1) Refaire une capture, comme dans l'exercice 5, mais cette fois-ci, en utilisant des outils se basant sur des transmissions cryptées (ssh).

2) Que remarque-t-on ?

**Exercice 8 : Capture sur un routeur**

1) Utiliser une machine de la salle ayant deux cartes réseaux pour en faire un routeur.

2) Configurer correctement les adresses IPs du routeur et des machines qui lui sont connectées.

3) Capturer, sur ce routeur, le trafic engendré par la commande ping (par exemple). Que remarque-t-on au niveau des adresses IP? des adresses MAC?

**Exercice 9 : Commande *netstat***

1) Utiliser la commande *netstat*. Qu'affiche cette commande ?

```
┌──(bamba㉿kali)-[~]
└─$ netstat
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
Sockets du domaine UNIX actives(sans serveurs)
Proto RefCnt Flags       Type       State         I-Node   Chemin
unix  2      [ ]         DGRAM                    24594    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM                    16595    /run/systemd/notify
unix  2      [ ]         DGRAM                    16611    /run/systemd/journal/syslog
unix  16     [ ]         DGRAM                    16617    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    16619    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTE      26619    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    20916
unix  3      [ ]         STREAM     CONNECTE      27919    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTE      24915    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTE      28203
unix  3      [ ]         STREAM     CONNECTE      25441    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTE      22327
```

netstat : Il livre des statistiques de base sur toutes les activités de réseau et donne par exemple des indications sur le port et l'adresse sur lesquels une connexion (TCP, UDP) est établie, mais également des indications sur quels ports sont ouverts pour des demandes.

2) Essayer les différentes options de la commande netstat, notamment celles permettant d'afficher les statistiques IP et TCP de la machine.

netstat -a : lister tous les ports (TCP et UDP) en état d'écoute

netstat -at : lister uniquement les connexions du port TCP (Transmission Control Protocol)

netstat -au : affiche toutes les connexions du port UDP (User Datagram Protocol)

netsat -r : permet d'afficher la table de routage IP du noyau