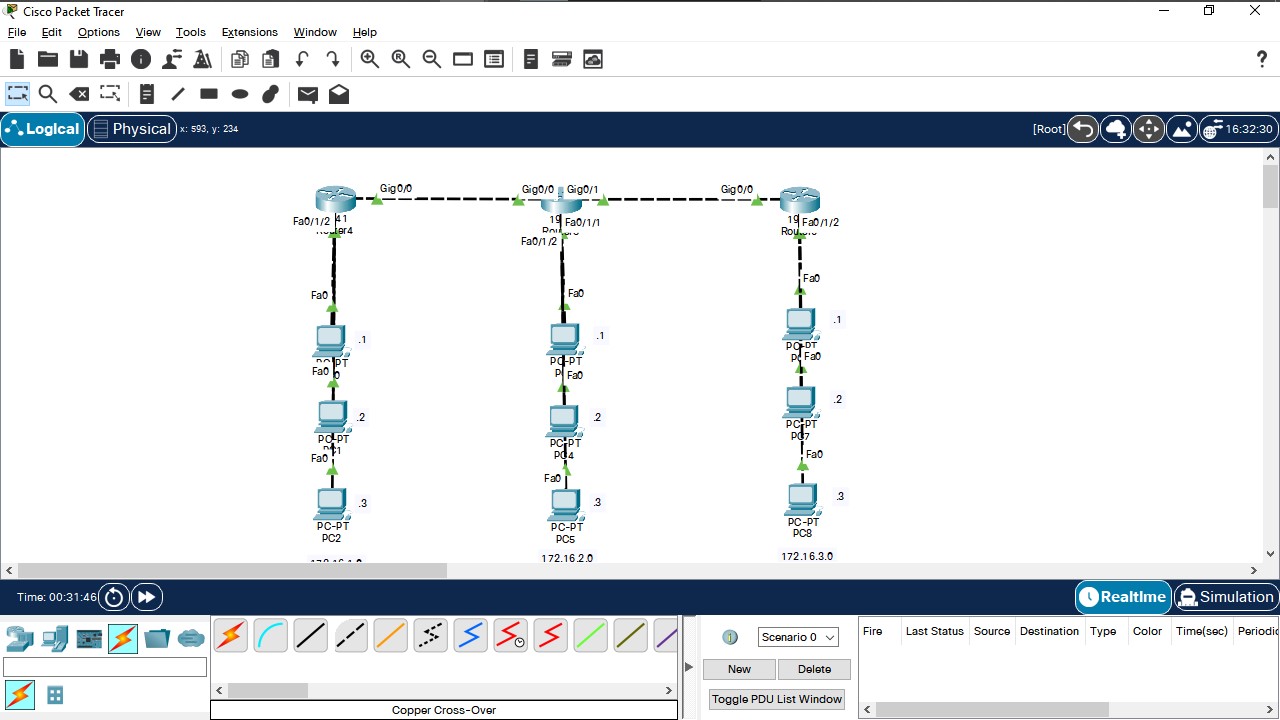
TPRESEAUUNIX

**- 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



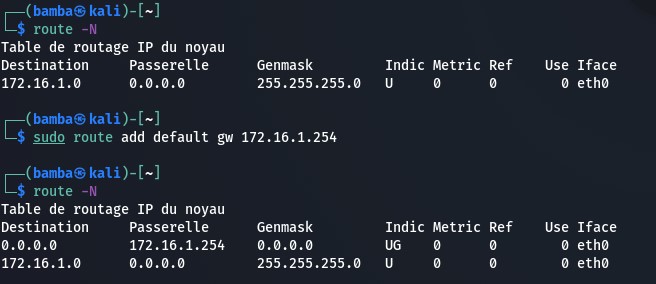
1. Indiquez pour chaque segment le type de câble nécessaire (droit ou croisé).

* 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.

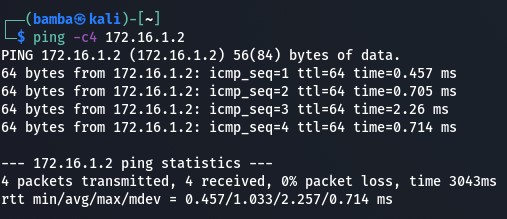


3) Utilisez la commande route pour configurer votre passerelle de sortie.

****

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

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

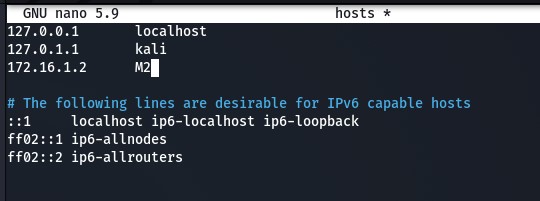


Nous ne pouvons pas utiliser le nom des machines а la place de l’adresse cas ils n’ont pas été définie

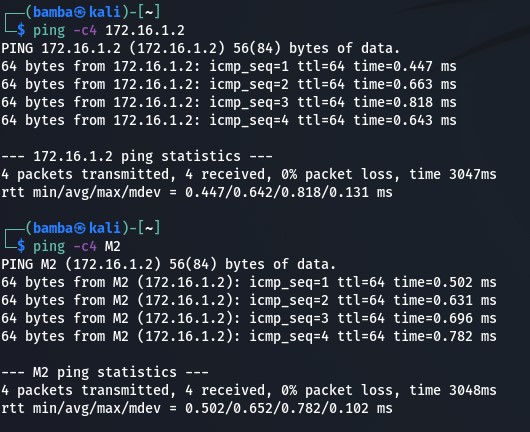
2) Utilisez le man pour trouver des informations sur le fichier /etc/hosts.



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



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



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

1) Il existe plusieurs commandes permettant de se connecter et d’utiliser а distance une

machine. Utilisez et indiquez les différences entre les commandes telnet et ssh.



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.

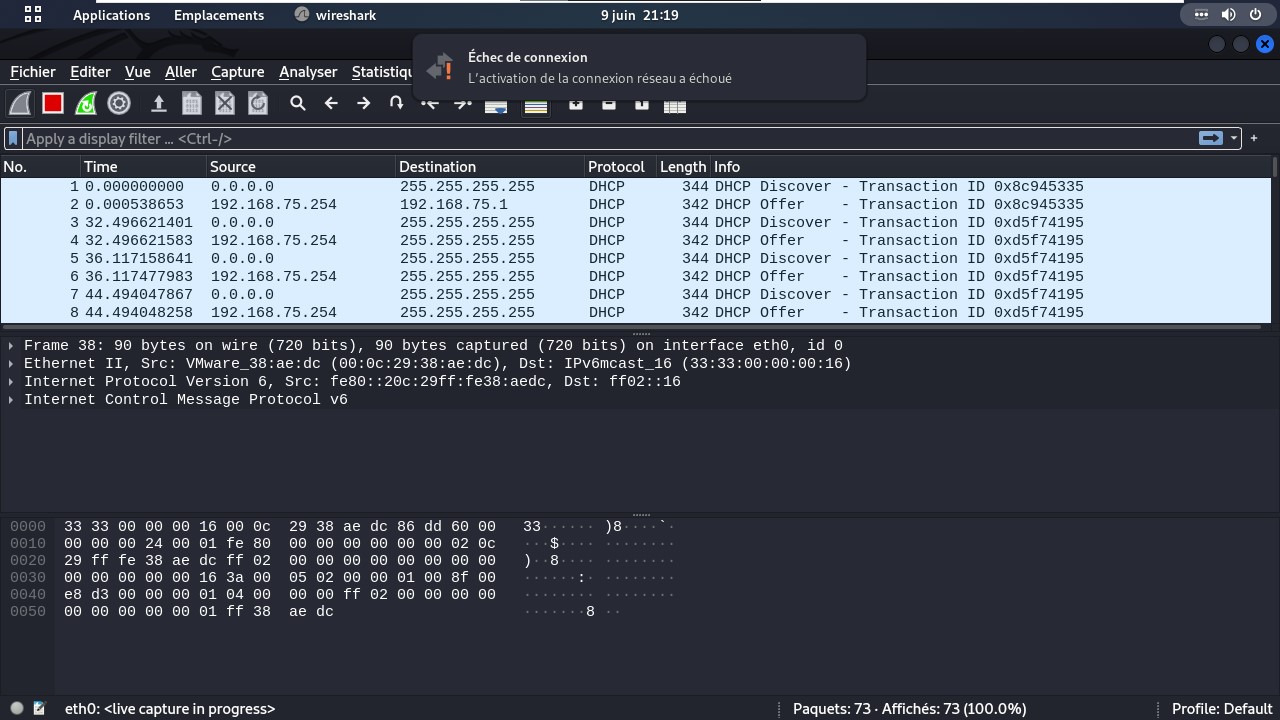
De plus, SSH utilise le cryptage à clé publique pour authentifier les utilisateurs distants, mais Telnet n’utilise aucun mécanisme d’authentification.

**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 а 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**

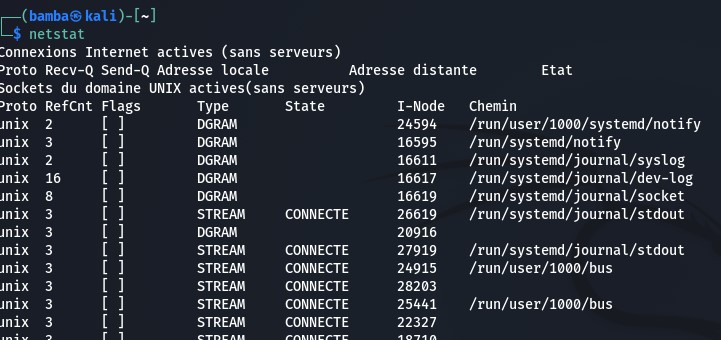
1) Utiliser une machine de la salle ayant deux cartes réseaux pour en faire un routeur.

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 ?



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