SCR.2.1 TP 14 ⊥ :

Les commandes `ip`, `nc/ncat/netcat`, `ss`, `tracepath/traceroute`

Les utilitaires `tcpdump`, `tshark/wireshark`

Rappel.

On n'utilise pas les commandes `ifconfig, arp, netstat, route`.

- L'utilitaire `tcpdump` permet de visualiser le trafic sur le réseau. Il donne une description du contenu des paquets sur une interface réseau. Cet utilitaire est un standard de toutes les installation Linux. Son utilisation est, par défaut, réservé à l'utilisateur root.
- L'application graphique `wireshark` permet aussi de décrire le trafic sur un réseau ; `tshark` en est la version ligne de commande.

↪ Aussi bien pour `tcpdump` que pour `tshark/wireshark`, les paquets dont on veut obtenir une description peuvent être filtrés par des expressions. On peut faire `man pcap-filter` pour avoir la manière de construire ces expressions.

↪ Aussi bien pour `tcpdump` que pour `tshark`, si on veut avoir le résultat, à la fois à l'écran et dans un fichier, on pipelinera avec la commande `tee <trace-file.txt>` (sans les `< >`, bien sûr.)

Filtre pour `tcpdump` et `wireshark`.

Il n'est pas pratique d'avoir les affichages polués par la description de paquets qui ne nous intéressent pas. Ainsi, avant de lancer la commande dont on veut analyser le traffic généré sur le réseau, commencer par "tailler" au mieux le filtre de `tcpdump/tshark`.

Pour cela, tester plusieurs lignes de commandes `tcpdump/tshark`, en réglant le filtre jusqu'à ce que `tcpdump/tshark` ne "parlent" que lorsqu'on aura soumis la commande dont on veut étudier le trafic généré. Par exemple, si on veut anlayser le traffic dû à un `ping` de A vers B, on ajoute dans le filtre l'expression `host <ip_A> and host <ip_B>` (sans les `< >`, bien sûr).

I. L'utilitaire `nc/ncat/netcat` permet, entre autres, de lancer des serveurs/clients.

1. Dans un terminal, lancer `nc` (ou le nom équivalent de l'utilitaire dont le lancement fonctionne sur sa machinee) en mode serveur udp sur un numéro de port assez élevé, disons 50000. Par la commande `ss`, vérifier que le serveur est bien lancé.
2. On va transmettre au serveur le contenu d'un fichier en utilisant une ligne de commande `nc` en mode client. On construit d'abord un fichier de la taille qu'on désire à l'aide de la commande `dd`. La valeur des octets dans le fichier ne nous intéresse pas. On peut donc utiliser le fichier spécial `/dev/zero` ou `/dev/urandom`, par exemple, comme source pour `dd`. Construire ainsi le fichier `ft-file.dat`, ayant comme taille, disons 9K octets (K=1024). Vérifier que le fichier obtenu a bien la taille voulue.

   Préparer une ligne de commande `tcpdump` réglée pour décrire ce qui se passera lorsqu'on aura lancé un client `nc` qui enverra le contenu du fichier `ft-file.dat` au serveur lancé précédemment.

3. Transférer le fichier `ft-file.dat` au serveur à l'aide de `nc` en mode client. En combien de paquets le transfert a-t-il été effectué ? Consulter les flags appropriés montrés par `tcpdump` et conclure s'il s'agit d'une fragmentation ou pas ?
4. On va refaire 3 mais en ayant lancé serveur et client sur deux machines différentes. On va préparer une ligne de commande `tcpdump` réglée pour analyser le trafic correspondant. Quelle option donnée à `tcpdump`
   (a) Si on ne veut pas alourdir l'affichage par les temps *timestamp* ?
   (b) Si on ne veut pas afficher ce qui se passe lors de la résolution des adresses mac ?
   (c) Si on veut les machines identifées uniquement par leur adresse ip (c'est à dire qu'on ne veut pas convertir vers les noms) ?
5. Lorsque l'expression qui filtre dans `tcpdump` est longue, on peut la placer dans un fichier dont on passe le nom à `tcpdump` à la ligne de commande. Quelle option de `tcpdump` utilise-t-on à cette fin ?
6. Maintenant, on se met en binôme et on lance un seul `nc` en mode serveur udp sur l'une des machines du binôme, appelons-la MS. Chaque membre du binôme prépare (sur sa machine) une ligne de commande `tcpdump` pour voir l'activité sur le réseau dûe au lancement d'un `nc` client qu'on va lancer uniquement sur la machine du binôme autre que MS.
7. Refaire 3. En combien de paquets le transfert a-t-il été effectué ? Y a-t-il une différence avec ce qu'on a obtenu en 3 ? Expliquer.

II. Les commandes `traceroute`/`tracepath` tracent la route empruntée par des paquets IP sur un réseau IP en direction d'un host donné pour découvrir la MTU le long de cette route.

1. Sans tenter de les lancer, vérifier si elles sont installées.
2. On prépare une ligne de commande `tcpdump` pour voir la description des paquets générés par le lancement de `traceroute` (ou `tracepath`). Ici, le filtre est plus compliqué. On ne sait pas, à priori quelles machines vont nous parler pendant qu'on trace la route. On peut déjà préciser que, dans les paquets voulus, on est source ou destination. Lancer une première ligne `tcpdump` et filter encore si des paquets sont décrits alors qu'on n'a pas encore lancé de commande. En utilisant le niveau de détail `-vvv` de `tcpdump`, repérer les protocoles encapsulés dans ces paquets indésirables et les retirer par une expression dans le filtre de `tcpdump`. Une fois qu'on est satisfait de la ligne de commande `tcpdump`, le niveau de détail donné par `-vv` suffit pour le reste. On recueillera le résultat dans le fichier `traceroute-trace.txt`.
3. Regarder la page du manuel de `traceroute` pour comprendre à quoi sert l'option `-n` . Dans un autre terminal, lancer un `traceroute` vers, disons `www.google.fr`, avec comme argument l'adresse IP et pas le nom.
4. À l'aide de `sed`, aérer le fichier contenant la trace, en insérant une ligne vide entre deux blocs consécutifs commençant par "IP". Maintenant, repérer, dans le résultat de la commande `traceroute`, une machine relais H qui n'apparaît pas plus d'une fois.
   (a) Repérer, dans le fichier trace, les identifiants des paquets auxquels H a répondu par un `"ICMP time exceeded in-transit"`. On peut faire `grep` sur l'adresse IP de H.
   (b) Avec quel `ttl` ces paquets ont été émis ? Comparer avec la position de H dans l'affichage donné par `traceroute`.
   (c) Quelle valeur de `ttl` ces paquets ont-ils à leur arrivée en H. Interpréter alors le message `"ICMP time exceeded in-transit"`.
   (d) Quels autres messages de ICMP voit-on dans la trace ? À quoi correspondent-ils ?