TP n°4 – ICMP (ping et traceroute)

1. ping

La commande *ping* utilise le protocole ICMP pour déterminer notamment si un nœud sur le réseau est accessible.
Lancez une capture sur Wireshark, puis tapez dans l'invite de commande : `ping www.unice.fr` puis `ping www.lemonde.fr`. Pour ne voir que les ping, tapez dans le filtre de recherche de Wireshark `icmp` (puis cliquez sur *Apply*). Lors d'un ping @IP, la machine locale va envoyer des `ICMP Echo Request` à @IP (aller) et attendre de recevoir des `ICMP Echo Reply` (retour) venant directement de @IP.

1. Quelles sont les informations données par cette commande ?

2. Quelles sont les adresses IP de ces deux sites ?

3. Qu'est-ce que le RTT ? Quels sont les RTT moyens pour ces deux `ping` ? Est-ce que vous avez des valeurs de RTT très différentes ou sont-elles du même ordre de grandeur ?

4. Quelles sont les valeurs données pour le TTL ? Quelles informations cela vous donne-t-il pour ces deux `ping` ? D'après vous, à quelle valeur a été initialisée le TTL lors de l'envoi de l'`ICMP Echo Reply`

5. Regardez les quatre requêtes d'écho successives, et identifiez les champs modifiés entre chaque requête.

6. Pourquoi les valeurs de la somme de contrôle ont-elles changé avec chaque nouvelle requête ?

7. Envoyez un ping vers 127.0.0.1, 127.255.254.2. Que recevez-vous ?

8. Comment sont différenciés les `Echo Request` des `Echo Reply` dans l'entête ICMP ? Quelles sont les autres valeurs possibles pour le champ que vous venez d'identifier.

9. Trouvez la valeur du MTU (plus grande taille de paquets que vous pouvez envoyer) utilisée en lançant la commande `ping -l xxxx -f @IP` où xxxx sera la valeur de MTU à trouver et @IP est l'adresse IP testée. L'option –f impose au paquet de ne pas être fragmenté, et lorsque le routeur devra le fragmenter, vous recevrez un message du type : `Le paquet doit être fragmenté mais est paramétré DF`. Trouvez donc la plus grande taille de paquet pour laquelle vous ne recevez pas ce message.

10. Est-ce que dans la capture de Wireshark réalisée, la taille du paquet est bien égale à celle que vous avez spécifiée dans votre commande ? Si non, essayez de comprendre d'où vient cette différence. Vous en déduirez la taille minimale d'un paquet ICMP et la taille de chacun des entêtes nécessaires pour l'envoi du paquet.

11. Vous regarderez comment sont remplis les paquets ICMP pour avoir la taille demandée, et vous remarquerez que les paquets avec une taille de MTU supérieure à celle trouvée précédemment ne sont pas capturés par Wireshark (avec l'option -f). Pourquoi ?

12. Lorsque vous enlevez l'option –f, et que vous essayez d'envoyer des ping de 65500 octets, cela va générer 45 paquets fragmentés. Trouvez leur taille. Pour cela, vous devez enlever le filtre icmp de Wireshark.

13. Quelles sont les autres options possibles pour la commande ping ? Testez certaines de ces options tout en lançant une capture Wireshark à chaque fois pour valider votre capture.

2. traceroute

La commande *tracert* utilise l'incrémentation du TTL pour indiquer quel est le chemin suivi par les paquets de la machine locale à l'hôte distant. En couche 4 (transport), le traceroute peut utiliser le protocole UDP, TCP ou ICMP. C'est cette dernière option par défaut qui est choisie par Windows.

1. Dans une invite de commandes, faites un *tracert* vers www.lemonde.fr tout en lançant une capture Wireshark. Regardez le nombre de routeurs traversés. Refaites plusieurs fois l'expérience pour observer éventuellement un changement de route.

2. D'après-vous comment fonctionne cette commande ? Vous pouvez comprendre son fonctionnement à l'aide de la capture Wireshark. Quels sont les paquets dans la capture qui indiquent les adresses des routeurs traversés ? il s'agit de messages d'erreur ICMP avec un code particulier.

3. Vous observez de temps à autre des * à la place de certains routeurs sur certaines captures. A quoi est-ce dû d'après-vous ?

4. Essayez de trouver ces mêmes routeurs en faisant varier le TTL de 1 à 30 avec la commande `ping`. Vous trouverez l'option nécessaire pour cela en tapant `ping` sans aucun paramètre dans votre invite de commandes.
5. Regardez l'adresse IP du premier saut sur plusieurs routes. Est-ce que cette adresse change ? à quoi correspond-t-elle ?

6. Le fichier `tracert.cap` vous indique une capture faite pour une commande traceroute. Vers quelle adresse IP a-t-elle était faite ? A quoi correspondent les paquets en noir ? Quel est le protocole utilisé pour cette commande traceroute ? Quelle est l'adresse IP de la passerelle par défaut sur laquelle se trouve la machine ? Quelle est son adresse mac ?

7. Vérifiez que c'est à chaque fois cette adresse mac que nous trouvons dans le champ adresse mac destination de l'entête ethernet pour toutes les requêtes icmp. Remarquez bien l'incrémentation du TTL dans les requêtes.

8. Le fichier `some-traceroute.pdf` présente des traceroute réalisés à l'aide de l'outil zenmap. La carte `traceroute-carte.pdf` a été réalisée à l'issue de ces captures. Trouvez les portions de route communes entre localhost (au centre du cercle) et les destinations serveurs (www.inria.fr, www.unice.fr, www.iut.unice.fr, www.yahoo.fr, www.lemonde.fr, www.google.fr, www.google.com). Localhost est situé à Sophia Antipolis chez un opérateur free, identifiez les villes par lesquelles la requête traceroute est passée pour aller jusqu'au serveur iut.unice.fr. Vous retrouverez notamment les routeurs Renater pour arriver jusqu'à cette adresse.

9. Faites les traceroute vers les mêmes adresses et vers des routeurs intermédiaires depuis votre poste de travail et regardez si vous retrouvez certaines adresses de routeurs ou certaines portions de route.