TD noté - Analyses Wireshark

Pascal Cotret, pascal.cotret@ensta-bretagne.fr

7 octobre 2022

Table des matières

Remarques

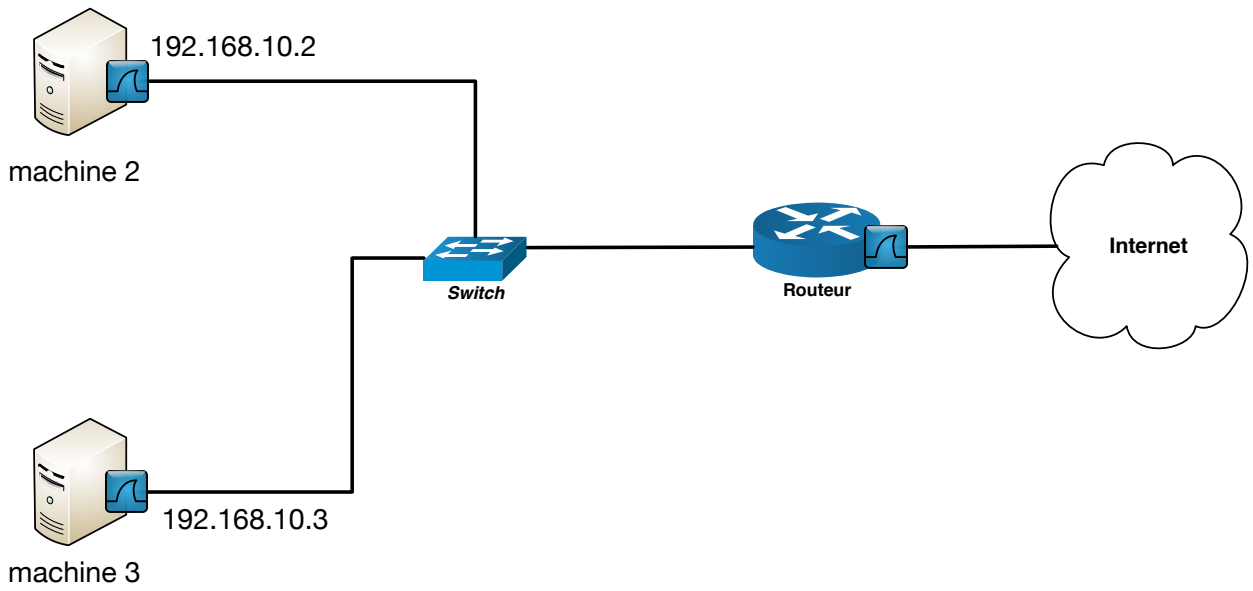
Les exercices 4 et 5 sont à question unique mais demandent un tout petit peu plus de recherche pour trouver la bonne information. Si vous n'êtes pas très à l'aise, traitez les à la fin.

Tous les exercices sont indépendants.

1 Analyse des trames d'un réseau local Ethernet

On considère le réseau illustré par la figure 1.

FIGURE 1 – Plan du réseau



Le logiciel Wireshark a été utilisé pour capturer le trafic à trois endroits distincts de ce réseau (matérialisés par les icônes Wireshark) : sur l'interface réseau de la machine 2, sur l'interface réseau de la machine 3 et sur l'interface du routeur qui le relie à Internet. Les captures réalisées en ces différents points correspondent respectivement aux fichiers `machine2.pcapng`, `machine3.pcapng` et `routeur.pcapng`.

On vous demande par la suite d'analyser le trafic contenu dans ces fichiers à l'aide de Wireshark afin de répondre aux différentes questions.

1.1 Exercice 1

Question 1. Dans le fichier `machine3.pcapng`, quel est le protocole utilisé au dessus de la couche IP dans le paquet #50 ? À quoi sert ce protocole ?

Question 2. Comment le destinataire de ce paquet peut-il déterminer le protocole de la couche réseau utilisé dans ce paquet, pour pouvoir le décoder ? Comment peut-il identifier le protocole utilisé au dessus d'IP ?

Question 3. Qui est l'émetteur de ce paquet ? Quelle est son adresse IP ? Quelle est son adresse MAC ?

Question 4. Quel est le message contenu dans ce paquet ? À quoi sert-il ?

Question 5. Qui est le destinataire de ce paquet ? Quelle est son adresse IP ?

Question 6. Quelle est l'adresse MAC de destination de ce paquet ? Correspond-elle au destinataire final de ce paquet ? Pourquoi ?

Question 7. Comment l'émetteur de ce paquet a-t-il pu déterminer l'adresse MAC du destinataire ? Expliquez le mécanisme à partir des échanges que vous pouvez observer dans la trace.

Question 8. Quel paquet contient la réponse au message contenu dans le paquet #50 ?

Question 9. Ouvrez maintenant le fichier `machine2.pcapng`. Quels sont les numéros des paquets correspondant aux messages identifiés dans les questions précédentes ? Est-ce que ces paquets sont identiques aux précédents (ont-il les mêmes adresses IP et MAC, source et destination) ? Pourquoi ?

Question 10. Ces paquets ont-il été envoyés au routeur ? Pourquoi ?

1.2 Exercice 2

Ouvrez de nouveau le fichier `machine3.pcapng`.

Question 11. Quel est le protocole applicatif utilisé par le paquet #78 ? À quoi sert-il ?

Question 12. Quel est l'émetteur de ce paquet (quelle est son adresse IP) ? Quel est le destinataire (quelle est son adresse IP) ?

Question 13. Quelle est l'adresse MAC destination de ce paquet ? Correspond-elle au destinataire final ? Pourquoi ?

Question 14. Comment l'émetteur de ce paquet a-t-il pu déterminer l'adresse MAC de destination ?

Question 15. Ce paquet a-t-il été envoyé au routeur ? Pourquoi ?

Question 16. Quel est le message contenu dans ce paquet ? À quoi sert-il ?

Question 17. Quel est le nom de domaine du destinataire de ce message ?

Question 18. En observant les paquets 71 à 74, expliquez comment l'émetteur a pu trouver l'adresse IP

du destinataire à partir de son nom de domaine.

Question 19. Quelle est la réponse à ce message ? Dans quel paquet est-elle transmise ?

2 Traceroute

Ouvrez avec Wireshark le fichier `traceroute.pcapng`. Comme son nom l'indique, il s'agit de l'enregistrement réalisé pendant l'exécution du programme `traceroute`.

Question 20. Filtrez la trace pour ne faire apparaître que les messages UDP. Identifiez le premier paquet UDP échangé. Quelle est son adresse IP source ? Quelle est son adresse IP destination ?

Question 21. À l'aide du site `https://www.ip-tracker.org/` ou d'un outil similaire, déterminez à qui appartient cette adresse IP. Dans quel pays est située la machine possédant cette adresse IP ? Quel est son nom de domaine ?

Question 22. Observez les champs de l'en-tête IP du premier paquet UDP. Quelle est la valeur du champ TTL ? À quoi correspond ce champ et à quoi sert-il ? Que risque-t-il de se produire pour ce paquet ?

Question 23. Comment évolue le champ TTL entre les paquets UDP successifs (vous devez analyser au moins les 7 premiers paquets) ?

Question 24. Supprimez maintenant le filtre d'affichage afin de faire apparaître de nouveau les messages ICMP. Identifiez le premier message ICMP (paquet #2). De quel type de message ICMP s'agit-il ? Quel est l'émetteur de ce paquet ? De qui s'agit-il ?

Question 25. Qui sont les différents émetteurs des messages ICMP suivants ?

Question 26. Pourquoi n'y a-t-il plus de messages ICMP entre les paquets UDP #49 et 52 ?

Afin de mesurer plus facilement le temps inter-paquet, cliquez avec le bouton droit de la souris sur la ligne des titres de colonnes de la zone centrale (celle indiquant No., Time, Source, etc.). Dans le menu déroulant, choisissez `Column preferences` et dans la fenêtre qui s'affiche, appuyez sur le bouton `+` pour ajouter une nouvelle colonne. Donnez lui un titre (par exemple RTT) puis modifiez son Type en `Delta time displayed`. Avec la souris, déplacez cette colonne en avant dernière position par un "glisser/déposer". Validez vos modifications.

Vous devriez maintenant voir s'afficher une nouvelle colonne. La valeur affichée dans cette colonne correspond au temps écoulé entre l'émission (ou la réception) du paquet précédent et la réception (ou l'émission) du paquet sélectionné.

Question 27. Comment évolue le temps entre les messages UDP et les messages ICMP correspondant ? Que se passe-t-il entre les messages 48 et 53 ?

3 Analyses diverses sur une capture Wireshark

Cet exercice est basé sur la capture Wireshark `exo4.pcapng`.

Question 28. Quel est le protocole principal (niveau réseau) utilisé pour des commandes telles qu'un `ping` ?

Question 29. Combien de requêtes `ping` dans cette capture ?

Question 30. Quelle est l'adresse IP de l'appareil avec l'adresse `08:00:27:4b:e3:60` ?

Question 31. Nous n'avons pas vu le protocole IGMP en cours... Malgré tout, pourriez-vous retrouver quelle version du protocole IGMP est utilisée dans cette capture ?

Question 32. Le protocole DHCP permet de configurer automatiquement une adresse IP pour une machine donnée. Si un utilisateur essaye de se connecter sur une machine, le nom de l'hôte passera par le protocole DHCP. Quel est le nom de l'hôte qui est à l'adresse 10.0.2.22 ?

Question 33. Quelle est l'adresse IP du serveur DHCP ?

4 Capture de pages web

Cet exercice est basé sur la capture Wireshark `trace-http.pcap`.

Question 34. Je suis allé sur plusieurs sites web. Quel est le premier site sur lequel je suis allé ? (bonus, quel est le premier fichier téléchargé)

5 Forensique des réseaux

Question 35. Ouvrez le fichier `covertinfo.pcap`.

— Que contient cette capture ? Quelque chose à signaler en particulier ?