Introduction

Ce TP fait appel à plusieurs outils et concepts abordés dans le cours et/ou via la plate-forme e-learning Cisco. Il traite de l''encapsulation et l'analyse des protocoles associés au modèle TCP/IP (notamment : ARP, ICMP, IP, TCP, UDP, DNS, HTTP).

Objectifs

- Utiliser quelques commandes de base systèmes et réseaux
- Etudier le fonctionnement des commandes de test de connectivité au niveau du LAN et Internet.
- Utiliser un analyseur de protocoles (wireshark)
- Analyser les données et flux résultant des commandes :
  - Address Résolution Protocol ou ARP; Protocole résolvant une adresse Ip en adresse phyique ou MAC.
  - Internet Control Message Protocol ou ICMP : Messages de type : Echo, Echo Reply et Time Exceeded.
  - Internet Protocol ou IP ; champ de l'en-tête IP : Time to Live. (ping, traceroute et tcptraceroute.)
  - Adressage matériel (MAC|Ethernet) et logique (IP).
  - Établissement, maintien et libération de connexion TCP : procédure en trois étapes, numéros de séquence et d'acquittement.
  - Requête et réponse HTTP.
  - Requête et réponse du service de noms de domaines (DNS).

Matériel et logiciel

- Un PC ou une machine virtuelle connecté au réseau du labo.
- Analyseur de protocoles Wireshark.

Compte-rendu de Tp et modalités de rendu

Le compte-rendu est une synthèse du travail effectué pendant la séance. Il vous permet de retenir ce que vous avez appris en effectuant les manipulations. Un compte rendu est avant tout un document de travail pour votre usage personnel. Il peut contenir les éléments suivants :

- Introduction, objectif du TP
- Précisez votre environnement de travail : matériel, logiciel, OS utilisés
- Description des différentes manipulations effectuées et leurs validations
- Conclusion, bilan des manipulations effectuées
- Attention à l'orthographe !

Le travail est à réaliser en binôme. Le compte-rendu de Tp est à déposer sur la plateforme moodle.

Date de remise: date de séance de TP + 7 jours.

1. *Analyse de Trames.*

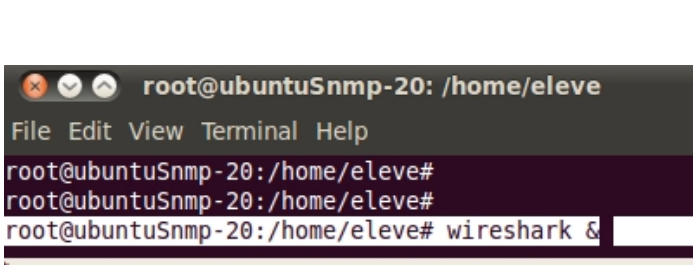
1.1. *Préliminaires*

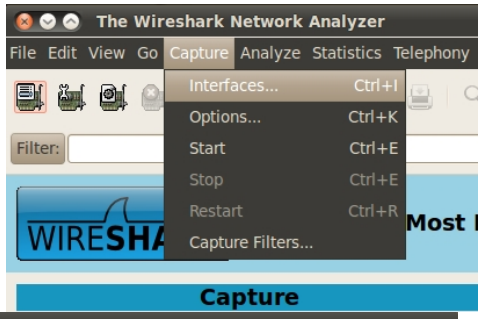
- Relever la configuration réseaux de votre station linux (ifconfig)
  Remarque : Il est probable que votre interface ait un numéro différent (ethX) de celle des voisins.

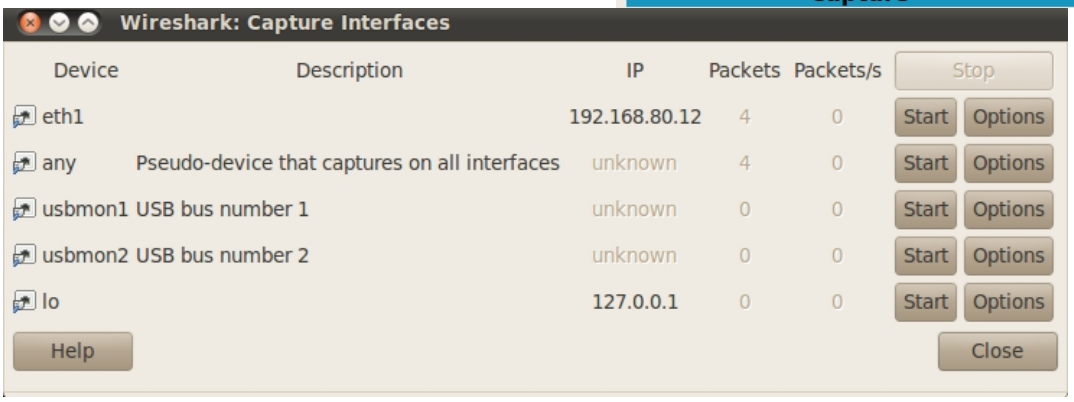
1.2. *Capture de trames*

1.2.1.Capture de flux associés à la commande ping

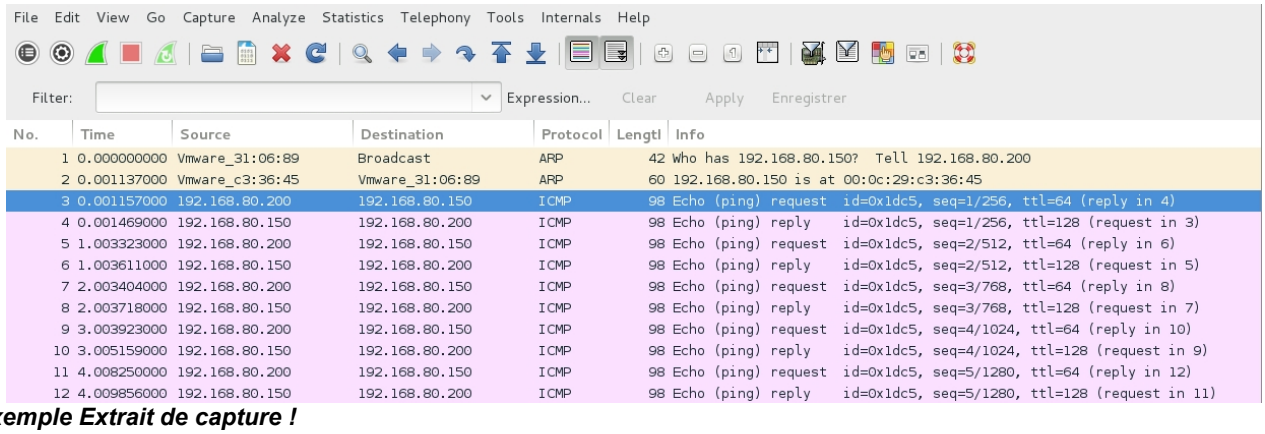
1. Ouvrir un shell et lancer Wireshark.
2. Sélectionner l'interface eth1 (cas de l'exemple). Lancer la capture des trames.







3. Lancer une console et exécuter les commandes
4. ping -c3 @IP_Poste_De_Votre_voisin_Ou_Autre_Adresse.
5. Arrêter la capture lorsque l'invite de commande réapparaît à la console.
6. Sauvegarder le fichier de capture1ping.



Exemple Extrait de capture !

1.2.2.Capture de flux associés à la commande traceroute

1. Lancer Wireshark.
2. Lancer la capture des trames
3. Lancer une console et taper une commande du type traceroute www.cisco.com
4. Arrêter la capture lorsque l'invite de commande réapparaît à la console.
5. Sauvegarder le fichier de capture2traceroute.

***Remarques** : La plage de ports UDP utilisée par défaut par la commande traceroute est de plus en plus fréquemment bloquée par les équipements d'interconnexion. Il est alors utile d'envisager l'emploi de la commande tcptraceroute avec laquelle on peut fixer les ports source et destination.*

1.2.3.Capture de flux associés à la commande tcptraceroute

1. Lancer Wireshark.
2. Lancer la capture des trames sans restrictions d'adresses, de protocoles ou de volume.
3. Lancer une console et taper une commande du type tcptraceroute -p 1024 www.phrack.org 80.

Bien sûr, le choix de l'adresse à contacter est totalement libre.

4. Arrêter la capture lorsque l'invite de commande réapparaît à la console.
5. Sauvegarder le fichier de capture3 tcptraceroute.

1.3. Analyse flux ARP et ICMP

Pour répondre aux questions suivantes, utiliser le résultat de la capture1ping issue de l'étape 1.1.1

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames Capturées ?
- Quelles sont les longueurs des messages échangés par les différents protocoles ?

1.3.1.Étude du paquet IP correspondant au premier message ARP Request.

❖ Caractéristiques Ethernet :

- Que transporte la trame Ethernet ?
- Quelle est l'adresse MAC source de la trame Ethernet ?
- Quelle est l'adresse MAC destination trame Ethernet ?
- Quelle est la signification de cette valeur ?

❖ Caractéristiques ARP :

- Quelle est la taille l'en-tete ? Quelle la taille des données transportées,
- Quelle est la valeur du champ Protocol Type contenu dans le message ARP?
- Quelle est l'adresse IP Source du paquet ARP?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est l'adresse MAC Source incluse dans le message ARP ?
- Quelle est l'adresse MAC destination incluse dans le message ARP ?

1.3.2.Étude du paquet IP correspondant au second message ARP Reply

❖ Caractéristiques Ethernet :

- Quelle est l'adresse MAC source de la trame Ethernet ?
- Quelle est l'adresse MAC destination trame Ethernet ?

❖ Caractéristiques ARP :

- Quelle est la taille l'en-tete ? Quelle la taille des données transportées,
- Quelle est la valeur du champ Protocol Type contenu dans le message ARP?
- Quelle est l'adresse IP Source du paquet ARP?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est l'adresse MAC Source incluse dans le message ARP ?
- Quelle est l'adresse MAC destination incluse dans le message ARP ?
- Quelle action effectue la station émettrice après réception du message ARP reply ?

1.4. Analyse du message ICMP

Sélectionner à la souris les octets de données du message de requête. Comparer ces données avec celles affichées dans la fenêtre d'affichage brut.

1.4.1.Message ICMP «Echo Request»

- Quelle est la taille l'en-tete ? Quelle la taille des données transportées,
- Quel est le type de message ICMP ?
- Quel est son identificateur ?
- Quel est le numéro de séquence ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est la valeur du champ Protocol Type ?
- Quelle est la valeur du champ Time to Live ?

1.4.2.Message ICMP «Echo Reply»

- Quel est le type de message ICMP ?
- Quel est son identificateur ? (A comparer à la requête question)

- Quel est le numéro de séquence ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est la valeur du champ Protocol Type ?
- Quelle est la valeur du champ Time to Live ?

1.4.3.Étude du message ICMP – Compléments

- Comparer ces données avec celles affichées dans le message de requête avec celles affichées dans le message de requête.
- Comment les champs d'identification et numéro de séquence évoluent dans le temps ?
- Est-ce que les séquences de données des requêtes et des réponses changent ?
- Calculer l'écart de temps entre l'émission de chaque message Echo Request et la réception de chaque message Echo Reply.
  Comparer les résultats avec les valeurs maximum, moyenne et minium fournies par la commande ping.

Remarque : *Linux affiche une autre valeur dans le résultat de la commande Ping qui est la déviation moyenne (mdev). Celle-ci est calculée avec les valeurs des temps de réponse. La déviation moyenne donne une indication à propos de la constance du temps de réponse. Autrement dit, une déviation moyenne basse signifiera que les valeurs des temps de réponse fournies par le Ping sont très similaires.*

1.5. Analyse avec (tcp) traceroute

Pour répondre aux questions suivantes, utiliser le résultat de la capture issue de l'étape précédente ou charger un fichier de capture.

1.5.1.Protocoles capturés

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ? Il est probable que les paquets ICMP soient précédés d'un jeu de questions/réponses DNS, UDP, ICMP.
- Relever l'adresse IP renvoyée avec la réponse DNS. @I associé à www.cisco.com

1.5.2.Message UDP

- Quelle est l'adresse IP destination du premier paquet contenant le message UDP
- Quelles sont les valeurs des champs Protocol Type et Time to Live ?)
- Comparer l'adresse IP destination relevée avec celle de la réponse DNS.
  Noter les valeurs caractéristiques de l'en-tête IP en vue d'une utilisation ultérieure.
- Combien d'octets de données sont présents dans ce message de requête ?

1.5.3.Message ICMP «Time Exceeded»

- Quelles sont les @ IP source et destination du paquet de la première réponse ICMP Time Exceeded ?
- Quel est le type de message ICMP ? (Les champs Type, message ICMP Echo Request.) Comparer les valeurs caractéristiques de cet en-tête avec celles notées ci-avant.
- Est-ce que le message ICMP contient de nouveaux octets de données ?

1.5.4.Evolution du champ TTL

- Combien de messages UDP sont émis avec la même valeur de champ TTL dans l'en-tête de paquet IP ?
- Quelles sont les adresses IP source des paquets ICMP Time Exceeded ?
  Comparer ces adresses avec celles données lors de l'exécution de la commande traceroute.
- Quel est le type du message ICMP reçu lorsque l'hôte destinataire est atteint ?
- Comment calculer les temps affichés par la commande traceroute à partir des valeurs données dans la colonne Time de la fenêtre des trames capturées ?

Remarque : Utiliser les pages de manuels de la commande traceroute pour obtenir la signification des différentes valeurs de temps pour atteindre une destination.

2. *Analyse flux Web (HTTP)*

2.1. Protocoles étudiés

- Adressage matériel (MAC|Ethernet) et logique (IP).
- Requête et réponse du service de noms de domaines (DNS).
- Établissement, maintien et libération de connexion TCP :
  - procédure en trois étapes, numéros de séquence et d'acquittement.
- Requête et réponse HTTP.

2.2. Marche à suivre

- Lancer Wireshark.
- Lancer la capture des trames sans aucune contrainte de filtrage.
- Lancer un navigateur Web et saisir l'adresse de site (URL) www.efrei.fr
- Une fois la page complètement chargée, arrêter la capture. Sauvegarder le fichier de capture, puis répondre aux questions suivantes.

2.3. Protocoles capturés

1. Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?

2. Quelle est l'utilité de la requête N°1 ?

2.4. Trame Ethernet, paquet IP et datagramme UDP

2.4.1. Analyser la trame correspondant au premier message DNS émis par le client Web.

3. Quels sont les adresses (MAC|Ethernet) et IP du client ?

4. Quel est le contenu du champ type de la trame Ethernet ?

5. Quelles sont les adresses destination (MAC|Ethernet) et IP ?

6. À quelles machines correspondent ces adresses ?

2.4.2. Analyser l'en-tête IP du premier message DNS émis par le client Web.

7. Quelle est la taille de l'en-tête ? Quelle est la longueur totale du paquet ?

8. Repérer le champ «type de protocole» dans l'en-tête. Quel est le numéro et le type de protocole présent dans les données du paquet ?

2.4.3. Analyser l'en-tête UDP du premier message DNS émis par le client Web.

9. Quels sont les numéros de ports du client et du serveur ? Quelles sont les particularités de ces valeurs ? Quel est le protocole de couche application présent dans les données du message ?

10. Quelle est la valeur indiquée dans le champ longueur de l'en-tête UDP ?
- Est-ce qu'elle correspond à l'information donnée dans l'en-tête du paquet IP ?
- Faire un croquis des piles de protocoles des couches physique à application pour le client et le serveur ;
- Identifier les unités de données de protocoles (PDUs) et les communications de bout en bout.

2.5. Service DNS

2.5.1. Analyser le message de requête DNS émis par le client Web.

11. Quel est le champ qui indique si le message est une requête ou une réponse ?

12. Quelle est l'information transportée dans le corps de la requête ? Identifier le type et la classe de la requête.

13. Quel est l'identificateur de transaction de la requête ?

On considère maintenant la réponse à la requête précédente.

14. Quelles devraient être les adresses (MAC|Ethernet) et IP de ce paquet ? Vérifier que les adresses attendues sont présentes.

15. Quelles sont les tailles du paquet IP et du message UDP ? Sont-elles supérieures aux messages requêtes ?

16. Quel est l'identificateur de transaction de la réponse ? Est-ce qu'il correspond à la requête ?

17. Combien de réponses sont disponibles dans le message de réponse ?
Comparer les réponses et leurs valeurs TTL (Time-to-live). Rep 1 Time to live = 3600 et time to live = 300

2.6. Connexion TCP

Identifier la trame qui correspond au premier segment TCP dans la procédure en trois étapes (three ways handshake) qui initie la connexion entre le client et le serveur HTTP.

18. Quelles sont les adresses (MAC|Ethernet) et IP attendues pour cette trame ?
- Quels sont les valeurs des champs type et protocole respectivement attendus pour cette trame et ce paquet ?
- Vérifier que ces champs et adresses correspondent.

19. Expliquer les valeurs des adresses destination (MAC|Ethernet) et IP ? À quels hôtes correspondent ces adresses ?

20. Identifier les numéros de ports utilisés par le client. Pourquoi ces valeurs sont-elles utilisées ?

21. Quelle est la longueur du segment TCP ?

22. Quel est le numéro de séquence initial (Initial Sequence Number ou ISN émis par le client vers le serveur ? Quelle est la taille de fenêtre initiale ? Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ?

23. Trouver la valeur hexadécimale de l'octet qui contient l'indicateur d'état SYN ?
Identifier la trame qui correspond au second segment TCP dans la procédure en trois étapes (three ways handshake).

24. Combien de temps s'est écoulé entre la capture du premier et du second segment TCP ?

25. Relever les valeurs des champs suivants de cette trame :
- Adresses MAC source et destination de la trame Ethernet.
- Adresses source et destination du paquet IP.
- Numéros de séquence et d'acquittement du segment TCP.
- Valeurs des indicateurs d'état. Verrier que tout correspond aux valeurs attendues.

26. Quelle est la longueur du segment TCP ?

27. Quel est le numéro de séquence initial (Initial Sequence Number ou ISN émis par le serveur vers le client ? Quelle est la taille de fenêtre initiale ? Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ? Identifier la trame qui correspond au dernier segment TCP dans la procédure en trois étapes (three ways handshake).

28. Combien de temps s'est écoulé entre la capture du second et du troisième segment TCP ?
- Comparer cette valeur avec celle relevée entre le premier et le second segment et expliquer la différence.

29. Relever les valeurs des champs suivants de cette trame :
- Numéros de séquence et d'acquittement du segment TCP ; Valeurs des indicateurs d'état ; Tailles de fenêtre.

30. Quelle est la longueur du segment TCP ?