IUT Béziers
Département Réseaux et Télécoms
B.U.T. R&T

2021/2022
R102
S.D.

R102 – Architecture des reseaux

Capture de trames / Protocole ARP

TP 1

> **Consignes**
> Vous allez, durant ce TP, devoir capturer et analyser des trames, ainsi que consulter le cache ARP de votre machine. Si vous utilisez ladite machine pour consulter des sites web ou rédiger votre compte rendu dans un cloud, cela risque de perturber les résultats obtenus. **Il vous est donc recommandé de ne pas utiliser d'applications en ligne pendant cette séance.**

1 Capture et analyse de trames

Exercice 1 Initiation a Wireshark

Lancer Wireshark pour effectuer des captures de trames sur votre interface Ethernet.

- ▷ Montrer comment filtrer le trafic pour n'avoir que les messages qui partent de ou qui arrivent à votre machine. On utilisera le champ filter.

- ▷ Capturer les trames émises et reçues lors de la consultation avec Firefox du site

  `http://www.perdu.com`

  Choisissez un des paquets HTTP échangés et donnez pour chaque couche du modèle TCP/IP :

  - ▷ Les protocoles utilisés pour cette trame
  - ▷ Les champs que vous comprenez du PCI de chaque couche

- ▷ Prenez l'un des paquets de votre choix. Dans son analyse en couches, une couche apparait tout en haut indiquant 'Frame XXX' où XXX est un numéro.

  A quelle couche du modèle TCP/IP correspond cette information ?
  Que contient-elle ?

Exercice 2 Analyse d'une trame ICMP Request

A l'aide de Wireshark, capturez les paquets émis par votre machine lorsque vous faites un ping vers une machine de la salle (Capturez jusqu'à la première réponse à votre ping)

Version du document
15 octobre 2021

- ▷ Quels paquets sont émis ? reçus ?
  Expliquez.

- ▷ Montrez l'encapsulation d'une trame ICMP-Request

Exercice 3 Follow TCP stream

Récupérez et ouvrez la capture effectuée par vos professeurs adorés à l'adresse suivante :

`http://www.lirmm.fr/~druon/assets/pdf/r102_tp1_capture.pcapng`

Vous pourrez, pour ce faire, utiliser la commande wget.

Cliquez avec le bouton droit sur le paquet numéro 923 de cette capture et sélectionnez "Follow TCP stream". Expliquez ce qui se passe. Comment Wireshark a-t-il réussi à isoler cette conversation des autres ?

Exercice 4 Graphique des flux

Toujours en analysant le fichier fourni, allez dans le menu Statistique et cliquez sur "Graphique des flux". Que voyez vous ? Explorez les autres analyses possibles.

Exercice 5 Analyse d'une trame Ethernet

Dans l'en-tête Ethernet quel champ permet de dire ce que contient la trame ?
Quelle est la valeur de ce champ dans le cas d'un paquet ARP ?

Exercice 6 Écriture d'un filtre sous Wireshark

Écrivez un filtre permettant de ne visualiser que les paquets :

- ▷ Émis par votre machine
- ▷ En TCP
- ▷ À destination du port 80

Testez votre filtre sur le fichier de capture téléchargé précédemment.

Quelle est l'adresse MAC de destination du paquet ?
Quelle est l'adresse IP de destination du paquet ? Expliquez.

Exercice 7 **Découverte de tcpdump**

Capturez avec tcpdump une requête HTTP vers le site `https://www.lawifi.fr`
Vous donnerez :

- ▷ Les actions et commandes effectuées
- ▷ La syntaxe du filtre permettant de faire la capture

2 La résolution ARP

L'objectif est de bien comprendre le fonctionnement du protocole ARP. Pour cela nous allons effectuer des captures de trames lors de résolutions classiques. On étudiera ensuite l'évolution du cache ARP d'une machine.

2.1 Fonctionnement du protocole ARP

Exercice 8 Affichez le cache ARP de votre machine à l'aide de la commande ip neigh.
Que contient-il ?

Exercice 9 A l'aide de Wireshark, capturez les paquets émis par votre machine lorsque vous faites un ping vers la machine de l'enseignant. (Capturez jusqu'à la première réponse à votre ping)

- ▷ Quelles trames émettez vous ?
- ▷ Quelles trames recevez vous ?
- ▷ Expliquez ce que vous observez en relation avec la question précédente.

Exercice 10 Affichez à nouveau le cache ARP de votre machine à l'aide de la commande ip neigh.
Que contient-il ?

Exercice 11 Effectuez à nouveau un ping vers la machine de l'enseignant et capturez les échanges.
Qu'observez vous ? Expliquez.

2.2 Observation du cache ARP

Consignes

Pour que vos relevés et vos paramètres ne soient pas perturbés par l'utilisation de votre navigateur web, il est recommandé de fermer toutes les applications inutiles pour le TP (navigateur web, etc.).

Exercice 12 Effectuez une requête ping vers votre voisin. Affichez de nouveau votre cache ARP.
Qu'observez vous ?

Exercice 13 Effectuez une requête ping vers un serveur en dehors du réseau de l'IUT. Affichez votre cache ARP.
Qu'observez vous ?

Refaites la manipulation avec un autre serveur extérieur. Qu'observez-vous ?
Pouvez-vous expliquer cela ?

Peut on avoir dans son cache une entrée avec l'adresse MAC du serveur `www.google.fr` ?
Expliquez pourquoi.

Exercice 14 Quel est le statut des entrées de votre cache ARP ? Qu'est ce que cela signifie ?

Exercice 15 Au bout de quelque temps, affichez votre cache ARP. Trouvez-vous toujours l'entrée correspondante au poste de votre voisin ?

Exercice 16

Contrôler la durée de vie du cache ARP

Dans le répertoire :

```
/proc/sys/net/ipv4/neigh/<interface reseau>/
```

Essayez de trouver le fichier qui gère la "durée de vie" d'une entrée du cache ARP et donnez sa valeur. Quels sont les autres variables et leur utilité ?

2.3 Modification du cache ARP

Il s'agit maintenant de modifier le cache ARP de votre machine afin de déclarer une machine de façon statique. Dans cette partie, nous prendrons comme exemple la passerelle.

Exercice 17

- ▷ Videz le cache ARP de votre machine. Si des entrées sont déclarées de façon statique supprimez les. Il faut que votre cache ARP soit vide.

- ▷ Effectuez une capture de trame lors d'un ping vers www.google.fr.

Quelles sont les entrées qui sont apparues dans votre cache ARP ?
Est-ce compatible avec votre capture de trame ?
Justifiez et illustrez vos propos avec des captures d'écran.

Exercice 18 Que se passe-t-il si vous refaites une tentative pour joindre www.tf1.fr au bout d'une minute ? Illustrez vos propos avec des captures de trames.
Quelle influence cela peut avoir sur le trafic réseau ?

Exercice 19 On va maintenant entrer l'adresse de la passerelle en statique dans le cache ARP. Récupérez l'adresse MAC de votre passerelle et entrez cette adresse de façon statique à l'aide de la commande *ip neigh* (voir man ip-neighbour)

Refaites une tentative pour joindre une machine de l'extérieur. Indiquez ce qui à changé en vous appuyant sur une capture de trame

3 Les switchs (partie optionnelle)

Exercice 20

- ▷ Connectez vous à l'interface d'administration de l'un des switchs Cisco 2960.
- ▷ Affichez la table de commutation du switch.
- ▷ Reliez votre switch au switch de la salle, et vos deux machines à votre switch.

Pinguez quelques machines présentes dans la salle. Affichez à nouveau la table de commutation et commentez.