IUT de Villetaneuse, Université Paris 13, Sorbonne Paris Cité 2017–2018
DUT R&T

M1104

TP

Vous noterez dans un compte-rendu à rendre à l'enseignant en fin de séance les réponses aux questions, les observations éventuelles ainsi que les commandes exécutées. Ce TP est à réaliser en binôme (un étudiant par machine) mais le compte-rendu est individuel. Une attention toute particulière sera portée à la présentation, aux explications et justifications.

Adresse MAC et adresse IP Chaque carte réseau d'une machine a deux adresses :
- MAC : est l'adresse physique qui est enregistrée dans la carte réseau.
- IP : est l'adresse logique qui est la seule connue et utilisée par les autres machines.

Dans ce TP vous utiliserez exclusivement l'interface `eth0` de votre machine.

Exercice 1: Outils de configuration de base

Action. Ouvrez un terminal et connectez-vous en tant qu'administrateur du système. Ensuite entrez la commande : `ethtool -K eth0 gso off tso off gro off`

Question 1 : Quelle est l'adresse MAC associée à votre carte `eth0` ? (Spécifiez la commande utilisée) Comment en déduisez-vous le constructeur de la carte ?

Action. Connectez vous à `www.coffer.com/mac_find` pour trouver le fabricant de la carte.

Question 2 : Quelle est votre adresse IP ? Quelle est sa classe ? Quel est le masque associé ?

Exercice 2: Wireshark

Wireshark est un programme de *capture de trames* : il communique directement avec une de vos cartes réseau qui lui transmet des informations sur les trames Ethernet qu'elle a transmises ou reçues. Wireshark peut ensuite détailler les différentes trames analysées en donnant par exemple, pour les trames Ethernet, la valeur de l'adresse de destination, le type du protocole, ...

Question 1 : Lancez le processus `wireshark` en tâche de fond (ignorez l'avertissement éventuel).

Action. Démarrez la capture de trame sur l'interface `eth0` en allant dans le menu `Capture`, en sélectionnant `Interfaces`, en cochant ensuite l'interface `eth0`, et en cliquant enfin sur le bouton `Start`. Attendez d'avoir reçu une cinquantaine de trames, et ensuite stoppez la capture.

Wireshark affiche les informations sur les trames capturées dans trois panneaux. Le panneau supérieur contient la liste des trames capturées (une ligne par trame) avec une brève description (adresses source et destination, type de protocole, ...) de ces trames. Le panneau du milieu détaille la trame sélectionnée dans le premier panneau. Enfin, le panneau du bas donne la trame complète sous forme hexadécimale.

Question 2 : Donnez les champs du PCI Ethernet que l'on retrouve dans la description des trames.

Question 3 : À quel protocole les PDU encapsulés dans Ethernet I appartiennent-ils ?

Question 4 : Comment fait `wireshark` à décider si une trame utilise Ethernet I ou Ethernet II ?

Exercice 3: Ping et ARP

Bien que les machines sur Internet communiquent avec leurs adresses IP, il est nécessaire à un moment donné d'encapsuler les messages échangés dans des trames Ethernet et donc de connaître l'adresse MAC de la machine que l'on souhaite contacter. On utilise alors le protocole ARP (*Address Resolution Protocol*) qui établit la correspondance entre les deux types d'adresses.

Nous allons étudier le principe de ce protocole simple en utilisant la commande `ping` utilisée pour tester si une machine est en marche et accessible. Le ping envoie un message du protocole ICMP au destinataire et si celui-ci est en marche et reçoit effectivement le message, il répond à l'envoyeur.

Action. Sur les deux machines du binôme, démarrez la capture de trame sur l'interface `eth0`. Dans une des machines, entrez la commande `ping -c1 <adresse>` où `<adresse>` est l'adresse IP de l'autre machine. Revenez ensuite sous `wireshark` et stoppez la capture de trames.

Question 1 : Donnez un chronogramme montrant la séquence des messages ARP et ICMP échangés lors de l'exécution entre votre machine et le destinataire du ping. Pour chaque trame, spécifier les adresses : MAC source et MAC destination qu'on trouve dans l'en-tête Ethernet, IP source et IP destination qu'on trouve dans le message ARP. Enfin, il conviendra d'expliquer en quelques phrases l'exécution du protocole étape par étape et le choix des adresses utilisées.

Question 2 : Sélectionnez la première trame ARP **reçue**.

1. Donnez la structuration de la trame ARP en faisant apparaître les différents PDU encapsulés.
2. Que vaut le champ `DL/Etype` du PCI Ethernet dans ce cas ? C'est la taille ou le type ?
3. Est-ce qu'il y a du bourrage ? Si oui, combien d'octets ?
4. Que peut-on en déduire sur la taille du SDU Ethernet ?

Question 3 : Sélectionnez la première trame ARP **envoyée**. Est-ce qu'il y a du bourrage ?

Question 4 : Sélectionnez la première trame ICMP envoyée.

1. Donnez la structuration de la trame ICMP en faisant apparaître les différents PDU encapsulés.
2. Est-ce qu'il y a du bourrage ? Pourquoi ?
3. Quelles sont les adresses IP source et destination ? Où trouve t-on ces informations ?
4. Quels sont le `type` et le `code` qui identifient le message `Echo-request` ? Où trouve t-on ces informations ?

Question 5 : Relancez la commande `ping` de la question précédente (sans lancer la capture de trames) puis entrez la commande `arp -n`. Qu'affiche-t-elle ?

Exercice 4: Le Protocole TCP

Action. Rédémarrez la capture de trame sur l'interface `eth0`. Dans le terminal, tapez la commande suivante :

```
wget http://www.iutv.univ-paris13.fr/index.php
```

Cette commande permet de télécharger le fichier à l'adresse indiquée sans ouvrir le navigateur. Nous l'utilisons uniquement pour générer du trafic et pouvoir capturer quelques trames. Revenez ensuite sur wireshark et stoppez la capture.

Question 1 : À quels protocoles appartiennent les PDUs encapsulés dans les trames Ethernet capturées ?

Question 2 :

1. Donnez la structuration des trames contenant des données HTTP (le contenu du fichier téléchargé, par exemple) en faisant apparaître les différents PDU encapsulés dans ces trames.
2. Quelles sont les tailles des PCI des différents protocoles utilisés pour transporter des données HTTP ?
3. Sachant qu'une trame Ethernet peut contenir au maximum 1500 octets de données, déduisez-en le nombre maximum d'octets de données HTTP que l'on peut trouver dans une trame Ethernet.

Question 3 : Sur Wireshark, mettez comme filtre `tcp` pour visualiser seulement les messages TCP. Quel protocole de niveau application utilise les services du protocole `TCP` ?

Question 4 : Donnez un chronogramme montrant la séquence des messages TCP échangés entre votre machine et la machine qui vous a envoyé les données HTTP. Expliciter les trois phases de connexion.

Question 5 : Les messages TCP sont ils acquittés ? Si oui, où on retrouve cette information ?

Exercice 5: Le Protocole UDP

Action. Rédémarrez la capture de trame sur l'interface `eth0`. (Ne pas oublier de supprimer le filtre TCP.) Dans le terminal, tapez la commande suivante :

```
nslookup 8.8.8.8
```

Cette commande permet de générer des datagrammes UDP. Stoppez ensuite la capture de trames.

Question 1 : Sur Wireshark, mettez comme filtre `udp` pour visualiser seulement les datagrammes UDP. Quel protocole de niveau application utilise les services du protocole `UDP` ?

Question 2 : Donnez un chronogramme montrant la séquence des messages UDP échangés lors de l'exécution de la commande.

Question 3 : Quels sont les SAP de niveau application que l'on trouve dans l'en-tête UDP ?

Question 4 : Est-ce qu' on trouve les phases d'ouverture et fermeture de la connexion ? Pourquoi ?

Question 5 : Les messages UDP sont-ils acquittés ? Si oui, comment ?