Création le : 11/06/2015
Quentin Giorgi.

TDM2 – Prise en main du réseau

Présentation du TP et travail préliminaire.

Vous disposez d'une station GNU/Linux sur laquelle une couche de communication protocolaire de type TCP/IP est installée.

Application
Transport (TCP,UDP,...)
Réseau (IP)
Liaison (Ethernet)
Physique (Ethernet)

Les couches Physique et Liaison sont principalement implémentées en matériel (carte réseau), les couches Réseau et Transport en logiciel (fourni par l'OS) et la couche application en logiciel.

Vous effectuerez des manipulations afin d'observer les échanges protocolaires, l'observation des protocoles s'effectuera via le logiciel wireshark qui intercepte les trames au niveau 2.

Vérifiez que vous avez une adresse IP sur l'interface eth0. Pour cela vous pouvez utiliser la commande « ip addr »

Premières manipulations, découverte de la station.

- Connectez-vous sur la station et lancez un terminal de commande, puis passez administrateur (nommé root) via la commande : « *su - »*

- A l'aide des commandes ci-dessous, répondez aux questions suivantes :

```
ip link
ip addr
ip route
```

- De combien d'interfaces ethernet disposez-vous ?

- Quelles sont les adresses MAC de l'interface physique connectée ? (niveau 2)
- indice : une adresse MAC se compose de 48bits.

- Quelle interface possède une ou plusieurs adresses IP (niveau 3), identifiez-les et donnez son nom ? - rappel : une adresse IP se compose de 32bits.

- Quel est la taille (en bit) du groupe de machines (aussi nommé sous réseau) auquel fait partie cette station, Quel est le numéro de votre machine dans ce groupe ?
- Demandez à votre voisin ces mêmes informations.

- Quelles sont les routes actuelles, à quoi correspondent-elles ?

- Quels réseaux permettent elles de joindre?

Observations de protocoles

Lancer un analyseur de réseau depuis un autre terminal via la commande « wireshark »

1 – Faites un test de connectivité vai la commande «ping 192.168.130.202 » sur le premier terminal

Observez les trames générées (vous pouvez appliquer un filtre ICMP), et sélectionnez des trames contenant des paquets de niveau 3 (IP) dont vous êtes source ou destination.

Quelles sont les encapsulations protocolaires observées?
Identifiez certains des champs des messages en rapport avec vos premières observations et répondez aux questions suivantes :

Dans quelle couche retrouvez-vous l'adresse MAC de la question précédente ?
Quelle est l'adresse MAC de la station destinatrice ?
De combien d'octets est constitué l'encapsulation protocolaire lié à cette couche ?

Dans quelle couche retrouvez-vous l'adresse IP de la question précédente ?
Quelle est l'adresse IP de la station destinatrice ?
De combien d'octets est constitué l'encapsulation protocolaire (entête) lié à cette couche ?
Citez trois autres champs de cet entête dont vous préciserez l'utilisation.

NOTE IMPORTANTE : Malgré l'encapsulation observée, ICMP n'est absolument pas un protocole de transport car il ne permet pas d'échanger des informations entre applications d'entités distantes, c'est un mécanisme de test de connectivité niveau 3.

Quelle leçon devez-vous en tirer ?

2- Enlevez le filtre ICMP, et lancez la commande :
dig in a www.esisar.grenoble-inp.fr

Recherchez dans wireshark les trames correspondantes à cette commmande.

Cette commande utilise t-elle une couche de transport ? Si oui laquelle ?
Quelle est l'adresse MAC de la station destinatrice ?
Quelle est l'adresse IP de la station destinatrice ?
L'encapsulation protocolaire liée à cette couche contient-elle beaucoup d'information ?
Retrouvez vous dans certaines trames la chaine « www.esisar.grenoble-inp.fr »

3- Enlevez le filtre, et lancez la commande suivante dans le terminal :
nc 192.168.130.211 80
puis tapez
GET / HTTP/1.0
(suivi de 2 fois la touche « return »)

Recherchez dans wireshark les trames correspondantes, identize une trame et avec le bouton droit faite « follow tcp stream. »

Cette commande utilise t-elle une couche de transport ? Si oui laquelle ?

Quelle est l'adresse MAC de la station destinatrice ?
Quelle est l'adresse IP de la station destinatrice ?
L'encapsulation protocolaire lié à cette couche contient-elle beaucoup d'information ?
Toutes les trames contiennent elles des données applicatives ?
Y a t-il des paquets échangés avec les deux entités avant d'envoyer des données ?

Pour les plus rapides

Sur une station dont vous connaissez l'adresse @IP faites la commande

nc -l -u -p 8080

Sur une autre station essayez de vous connecter avec la commande

nc -u @IP 8080

Observez les trames issues de cette demande de communication. Comment les adresses MAC permettant l'échange de trames sont elles connues ?

Y a t-il un lien avec le résultat de la commande :

arp -an ou ip neighbor