TP - Analyse de trame

M. Tellene

I Rendu

Le TP comporte des questions. Les réponses devront être rendues dans un fichier pdf sur moodle à la fin de la séance. Vous devrez joindre, aux moments indiqués, des captures d'écrans de *Wireshark*.

II Un peu de cours

Deux cartes réseaux qui communiquent s'échangent des messages (suite d'octets) appelés **trames**. Tous les postes connectés au même câble reçoivent le message, mais seul celui à qui il est destiné le lit.

Comment sait-il que cette trame lui est adressée ? Car il reconnaît l'adresse de destination, contenu dans la trame comme étant la sienne.

Comment sait-il qui lui a envoyé la trame ? Car la trame contient aussi l'adresse de l'émetteur.

L'adresse correspond à l'adresse de la carte réseau. On parle d'adresse physique car elle est physiquement liée au matériel, elle écrite sur la *PROM* (Programmable Read-Only Memory).

II/1 Notion d'adresse logique et de paquets

Que se passe-t-il si on change de carte réseau sur un poste ? L'adresse d'une carte réseau correspond à l'adresse d'un poste et d'un seul. Or les postes sont généralement regroupés en réseau.

Comment identifier le réseau auquel appartient le poste ? Il faut une adresse logique qui soit indépendante de l'adresse physique. C'est ce que proposent le protocole `IP` et le protocole `IPX` (*Internetwork Packet Exchange*). Ici nous verrons `IP`.

Pourquoi identifier le réseau ? Pour permettre à 2 postes qui ne sont pas connectés au même réseau de communiquer. Cela est impossible avec une adresse `MAC`, il faut une adresse de niveau supérieur, comme nous le verrons un peu plus loin et surtout avec **le routage**. Ce qu'il nous faut savoir à ce stade, c'est qu'une machine sait que le paquet n'est pas destiné au réseau si l'adresse réseau de destination est différente de la sienne, dans ce cas elle envoie le paquet à une machine spéciale dont le rôle est d'acheminer les paquets qui sortent du réseau (cf. la passerelle par défaut).

II/2 Étudions l'adresse `IP`

Une adresse `IP` a une longueur de 32 bits. Elle se compose d'une partie réseau et d'une partie adresse du poste sur le réseau. Il existe aussi en `IP` des adresses de multicast et de broascast.

L'adresse `IP` est logique, lorsqu'on change la carte réseau, l'adresse `IP` du poste ne change pas. En `IP` lorsqu'un poste envoie un message à un autre poste, il met son message dans un paquet précédé de

l'adresse IP du destinataire avec son adresse IP d'émetteur. Mais les cartes réseaux ne lisent pas les adresses IP, **elles ne lisent que les adresses** MAC.

Pour pouvoir être correctement transmis, le paquet va être mis dans une trame avec une adresse MAC de destination et une adresse MAC d'émission. On dit qu'un paquet IP est **encapsulé** dans une trame. Mais pour que tout cela fonctionne, il faut un mécanisme qui permettra de passer d'une adresse logique à une adresse physique, et vice-versa. C'est ce que nous allons étudier maintenant.

III Partie pratique

III/1 Structure du réseau

Le réseau que nous allons construire est pour le moment simpliste, mais il va vite devenir complexe d'autant qu'il est virtuel. Pour ce TP, il faudra créer 2 machines virtuelles Windows et les mettre sur réseau isolé du reste des machines.

III/2 Paramétrage d'une machine

Pour ce TP, vous devrez créer deux machines Windows (édition professionnelle de Windows). Dans un premier temps, créer la première machine en la mettant dans un dossier **SRV1**. Cette machine **devra s'appeler SRV1** (*attention modifier le nom de la machine sur VirtualBox n'est pas suffisant, il faudra également aller dans les paramètres système de la machine une fois que cette dernière sera démarrée*).

Note : respecter les noms des machines donnés (**SRV1**, **WS1**) car il y sera fait référence plus tard.

III/2.b Caractéristiques de SRV1

Avant de lancer la machine **SRV1**, vérifier que les caractéristiques suivantes sont bien respectées :

- 4Go RAM
- 50Go HD
- **Réseau interne** (permet de créer un réseau virtuel isolé, où les communications seront possibles uniquement entre les machines virtuelles connectées sur un même réseau interne. Ce mode d'accès réseau est intéressant pour reproduire un vrai réseau puisque l'on isole totalement ce réseau virtuel des autres réseaux.)
- nom : **SRV1**
- **Une fois que la machine est lancée**, adresse `IP` : `192.168.1.1`

TODO : Mettre une capture d'écran montrant le changement du nom de SRV1 et le mise en place de l'adresse `IP`

III/3 Installation de la seconde machine

La seconde machine virtuelle devra être sauvegardée dans un dossier **WS1**. Cette machine **devra s'appeler WS1** (*attention là aussi modifier le nom de la machine sur VirtualBox n'est pas suffisant*).

III/3.c Caractéristiques de WS1

Avant de lancer la machine **WS1**, vérifier que les caractéristiques suivantes sont bien respectées :

- 2Go RAM
- 40Go HD
- VMnet2
- nom : **WS1**
- **Une fois que la machine est lancée**, adresse `IP` : `192.168.1.10`

TODO : Mettre une capture d'écran montrant le changement du nom de SRV1 et le mise en place de l'adresse `IP`

III/4 Tester la présence d'un poste sur le réseau avec la commande `ping`

Les manipulation suivantes sont à faire sur **WS1** :

1. Ouvrir la fenêtre d'**invite de commande** et tapez `ipconfig`. Faire une capture du résultat
2. Tester l'adresse `IP loopback` pour vérifier que les liaisons définies par `TCP/IP` sont correctes : `ping 127.0.0.1`. Faire une capture du résultat
3. Tester un `ping` avec l'adresse `IP` de votre poste physique. Faire une capture du résultat
4. Tester un `ping` avec l'adresse du serveur. Faire une capture du résultat
5. Tester un `ping` avec l'adresse du réseau : `192.168.1.0`. Faire une capture du résultat. Vous indiquerez ce que signifie la réponse.
6. Tester un `ping` avec l'adresse de broadcast sur ce réseau : `192.168.1.255`. Faire une capture du résultat. Vous indiquerez ce que signifie la réponse.
7. Tester une adresse au hasard ne faisant pas partie du réseau : `200.110.20.37` Que pouvez-vous déduire du résultat?

   Par défaut, le pare-feu Windows interdit la réponse au `ping` (protocole `ICMP`), il faut donc modifier les réglages du pare-feu à la fois sur **WS1** et sur **SRV1** ; le mode opératoire est décrit dans le document **Utilisation du pare-feu pour le ping.pdf**

8. Après avoir fait les modifications adéquates sur **SRV1** et **WS1**, tester un `ping` vers le serveur. Faire une capture du résultat

III/5 Les commandes `ARP`

La commande `arp /?` donne une aide :

```
C:\Users/admin>arp /?

Affiche et modifie les tables de traduction des adresses IP en physique
utilisées par le protocole de résolution d'adresses ARP.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Affiche les entrées ARP actives en interrogeant les données en
            cours du protocole. Si adr_inet est spécifié, seules les
            adresses IP et physiques de l'ordinateur spécifié sont
            affichées. Si plus d'une interface réseau utilise ARP, les
            entrées de chaque table sont affichées.
-g          Identique à -a.
inet_addr   Spécifie une adresse internet.
-N if_addr  Affiche les entrées ARP pour l'interface réseau spécifiée par
            if_addr.
-d          Efface l'hôte spécifié par inet_addr.
-s          Ajoute l'hôte et associe l'adresse Internet inet_addr avec
            l'adresse physique eth_addr. L'adresse physique est donnée sous
            la forme de 6 octets en hexadécimaux séparés par des tirets.
            L'entrée est permanente.
eth_addr    Spécifie une adresse physique.
if_addr     Spécifie l'adresse Internet de l'interface dont la table de
            traduction des adresses devrait être modifiée. Non précisée,
            la première interface applicable sera utilisée.
```

— `inet_addr` : représente une adresse `IP`

— `eth_addr` : représente une adresse `MAC`

— `if_addr` : représente le numéro de la carte réseau (1, 2 ...)

Note : quand on parle d'hôte on désigne soit un ordinateur, soit une imprimante ou tout autre dispositif équipé d'une carte réseau.

III/5.e Remplir le cache automatiquement

1. Sur **SRV1**, noter l'adresse *Ethernet* de **SRV1**
2. Sur **WS1**, vider le cache `ARP`. Quelle commande vous a permis de réaliser cette action ?
3. Sur **WS1**, afficher le cache `ARP`
4. Sur **WS1**, tester la commande `ping 192.168.1.10`. Le ping fonctionne-t-il ?
5. Sur **WS1**, afficher le cache `ARP`. Est-il différent comparer à avant l'envoi du `ping` ? Si oui, expliquer pourquoi ? Aide à la question.

III/6 Utilisation de *Wireshark*

— Télécharger *Wireshark* (https://www.wireshark.org) sur **SRV1**. Pour ce faire, il faudra repasser en **NAT** et mettre une adresse automatique sur **SRV1**. Une fois l'installation finie, vous remet-

trez **SRV1** en **réseau interne** et lui redonnerez l'adresse IP adéquate

Instalation de Wireshark : Faire *Next* > *Noted* > *Next* > *Next* > *Next* > *Next* > ***Si ce n'est pas coché, cocher « Install NpCap 1.XX »*** > *Next* > *Install*. Pendant l'installation, une fenêtre va s'ouvrir, faire *I Agree* > ***Cocher Install NpCap in WinPcap API-compatible Mode »*** > *Install*. Une fois l'installation finie, faire *Next* > *Finish*. La fenêtre précédente se rouvre, une fois l'installation finie, faire *Next* > *Finish*

— Démarrer *Wireshark* **sur SRV1**
— Sélectionner la carte à regarder, la capture devrait commencer
— Générer du trafic réseau : sur **WS1**, vérifier que le cache ARP est vide, s'il ne l'est pas le vider. Faire un ping sur l'adresse IP du serveur **SRV1**

— Une fois le ping terminé, arrêter la capture des données réseau

Après avoir arrêté la capture, on obtient l'écran suivant :

2	35.976233	PCSSystemtec_22:6f:…	Broadcast	ARP	60 Who has 192.168.1.1? Tell 192.168.1.10
3	35.976251	PCSSystemtec_84:e2:…	PCSSystemtec_22:6f:…	ARP	42 192.168.1.1 is at 08:00:27:84:e2:30
4	35.976478	192.168.1.10	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=57/14592, ttl=128
5	35.976570	192.168.1.1	192.168.1.10	ICMP	74 Echo (ping) reply id=0x0001, seq=57/14592, ttl=128
6	36.995984	192.168.1.10	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=58/14848, ttl=128
7	36.996095	192.168.1.1	192.168.1.10	ICMP	74 Echo (ping) reply id=0x0001, seq=58/14848, ttl=128
8	38.010399	192.168.1.10	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=59/15104, ttl=128
9	38.010505	192.168.1.1	192.168.1.10	ICMP	74 Echo (ping) reply id=0x0001, seq=59/15104, ttl=128
10	39.026366	192.168.1.10	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=60/15360, ttl=128
11	39.026438	192.168.1.1	192.168.1.10	ICMP	74 Echo (ping) reply id=0x0001, seq=60/15360, ttl=128

1. Cliquer sur la première ligne
2. La liste des protocoles embarquées dans cette trame apparaissent sur la partie basse. Il devrait y avoir *Frame, Ethernet II* ainsi que *Address Resolution Protocol*
3. Développer le détail *Ethernet*
   (a) Quelle est l'adresse de destination ?
   (b) Pourquoi c'est cette adresse ? Faire un lien avec la table ARP de **WS1**.
   (c) Quelle est l'adresse source ? A qui appartient cette adresse ?
   (d) Quel est le code hexadécimal et le type contenu dans la trame *Ethernet* ?
   (e) A l'aide des informations recueillies, indiquer quelle est la longueur totale de l'entête.
   (f) En vous aidant de la présentation du protocole ARP, indiquer quelle devrait être la longueur de la zone données ?
   (g) Pourquoi la zone donnée de la trame Ethernet contient-elle 46 octets ?
   (h) Par quoi la zone donnée de la trame Ethernet a-t-elle été complétée ?

III/7 Étude du protocole ARP

1. Développer le détail *Address Resolution Protocol*
   (a) A quelle opération ARP cette trame correspond t-elle ? Dans quel champs peut-on avoir cette information ?
   (b) Pourquoi l'adresse matérielle de la cible contient des zéros ?
   (c) Comment la machine de destination peut-elle se reconnaître si la trame est envoyée en diffusion sur le réseau ?

2. Sélectionner maintenant la seconde ligne de la trace et développer le détail de *Address Resolution Protocol (Reply)*
   (a) L'adresse MAC de destination est-elle toujours 00:00:00:00:00:00 ? Expliquer pourquoi.

III/8 Exament de paquets ICMP

Rappel : ICMP (*Internet Control Message Protocol*) est un protocole de contrôle des flux, il permet d'une part de déterminer l'état des connexions entre deux machines (PING) et d'autre part de détecter les erreurs dans l'échange de datagrammes. Les messages ICMP sont encapsulés dans le protocole IP.

Maintenant que la machine destination a indiqué quelle était son adresse physique, le ping va envoyer des données à l'adresse IP de la machine de destination et attendre le retour. Elle va ainsi pouvoir mesurer la rapidité et fiabilité du dialogue avec cette machine sur le réseau.

Pour effectuer ces allers-retours, ping utilise le protocole ICMP. Pour le moment nous laisserons de côté l'étude d'IP pour nous concentrer sur ICMP.

1. Cliquer sur la première trame ICMP dont la colonne de description contient l'entrée `Echo (ping) request`

   Les protocoles encapsulés sont : *Trame*, *Ethernet II*, IP et ICMP

2. Développer le détail d'*Internet Control Message Protocol*

   (a) Quelle est la valeur hexadécimale de Type ? A quoi cela correspond ?

   (b) Data concerne les données envoyées au destinataire, elles devront être retournées telles quelles à l'expéditeur. Qui y a-il dans ces données et sur quelle longueur ?

3. Cliquer sur la deuxième trame ICMP dont la colonne description contient l'entrée `Echo (ping) reply` et développer le détail d'*Internet Control Message Protocol*

   (a) Quelle est la valeur hexadécimale de Type ? A quoi cela correspond ?

   (b) Qui y a-il dans le champs Data ? Quelle est la longueur ?

4. Examiner successivement les trames `Echo (ping) request` et `Echo (ping) reply` suivantes.

   (a) Combien y a-t-il de trames `Echo (ping) request` en tout ?

   (b) Combien y a-t-il de trames `Echo (ping) reply` en tout ?

5. Cela correspond-il avec l'écran du poste **WS1** ?