

Compte Rendu TP 2 Reseaux

Ute Abel
Colm Ryan
Emmanuel Stone

March 23, 2004

Abstract

Ce compte rendu explique le déroulement du TP2 réseaux.
On observe les différents protocoles utilisés avec des réseaux.

1 Le protocole ARP

1.1 Syntaxe des paquets ARP

On a vidé les tables ARP sur les deux machines, et après l'exécution de ping, on a constaté que la table ARP de la machine A contient l'adresse de la machine B et vice versa.

Table ARP en A :

```
195.221.226.44 at 00:b0:d0:5c:5b:55 on x10  
195.221.226.45 at 00:b0:d0:5c:5a:bd on x10
```

Table ARP en B :

```
195.221.226.45 at 00:b0:d0:5c:5a:bd on x10
```

Le délai de vidage automatique dépend du système d'exploitation; dans ce cas-là, il était d'approximativement 20 minutes (on croit).

1.2 Structure d'un paquet ARP

Le contenu des paquets voir avec 'Ethereal':

```
Frame 1 (60 bytes on wire, 60 bytes captured)
  Arrival Time: Mar  9, 2004 08:21:44.324130000
  Time delta from previous packet: 0.000000000 seconds
  Time relative to first packet: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 60 bytes
  Capture Length: 60 bytes
Ethernet II, Src: 00:b0:d0:5c:5a:bd, Dst: ff:ff:ff:ff:ff:ff
  Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Source: 00:b0:d0:5c:5a:bd (00:b0:d0:5c:5a:bd)
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000...
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:b0:d0:5c:5a:bd (00:b0:d0:5c:5a:bd)
  Sender IP address: 195.221.226.45 (195.221.226.45)
  Target MAC address: 2e:2f:30:31:32:33 (2e:2f:30:31:32:33)
  Target IP address: 195.221.226.44 (195.221.226.44)
```

```
0000  ff ff ff ff ff ff 00 b0 d0 5c 5a bd 08 06 00 01  .....\Z.....
0010  08 00 06 04 00 01 00 b0 d0 5c 5a bd c3 dd e2 2d  .....\Z....-
0020  2e 2f 30 31 32 33 c3 dd e2 2c 00 00 00 00 00 00  ./0123...,.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Ceci la structure d'un paquet ARP:

```
[ 64 ] [ 48 ] [ 48 ] [ 16 ]  
preamble destination source type  
+  
marqueur debut (adresse MAC) (adresse MAC)
```

Le quatrième champ "type" permet d'identifier le paquet comme étant de type ARP. Le paquet ARP se situe au début de la trame Ethernet. La valeur du champ "type" permet aussi d'estimer la taille du paquet qui vient d'arriver. La fin du paquet est soit ne pas marqué du tout (donc la disparition du signal détection de porteuse indique la fin du paquet) ou par le mot IP ajouté la fin. La couche Ethernet transmet la couche ARP l'information qu'un paquet du type ARP été reçu. Il appartient donc au protocole ARP d'évaluer l'information reçue avec ce paquet, c'est dire, de comparer l'adresse internet recherché par la station qui a émis la requête avec l'adresse internet de la station. Si elles sont identiques, une réponse sous forme d'un paquet ARP contenant l'adresse physique recherché est émise. Ethernet est au courant d'un bourrage avant la réception d'un paquet; si la station emettrice détecte une collision, l'émission en cours est remplacé par des bits de bourrage pour avertir les autres stations.

A quoi sert le protocole ARP? Le protocole ARP gère la communication des ordinateurs sur un réseau; plus exactement, il aide la station émettrice à faire le lien entre l'adresse Internet et l'adresse physique de la station cible. Si l'adresse Internet d'une station existe déjà comme entrée de la table ARP, on peut y trouver l'adresse physique correspondante. Sinon, une requête (contenant l'adresse internet de la station cible et l'adresse physique de la station source) sous forme d'un paquet ARP est envoyé chaque station active du réseau; la station qui reconnait sa propre adresse internet renvoie son tour son adresse physique. Toutes les deux enrégistrent le couple "adresse internet / adresse physique" de l'autre station dans leur table ARP.

Comme l'adresse physique d'un ordinateur dépend de la carte réseau (qui peut-être échangé après un temps) et pour éviter le stockage d'informations obsolètes, les entrées de la table ARP sont effacées périodiquement.

2 Le protocole ICMP

Le paquet ICMP qui été envoyé pas le logiciel 'send_icmp'.

```
x08 x00 x00 x00 xa6 x00 x00 x00 x5d x70 x4d x40 x9f x40 x0c x00 x08
  x09 x0a x0b x0c x0d x0e x0f x10 x11 x12
x13 x14 x15 x16 x17 x18 x19 x1a x1b x1c x1d x1e x1f x20 x21 x22 x23
  x24 x25 x26 x27 x28 x29 x2a x2b x2c x2d x2e x2f x30 x31 x32 x33 x34
  x35 x36 x37
```

L'entete de paquet observé dans le reseau avec 'Ethereal':

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x110b (correct)
  Identifieur: 0xa600
  Sequence number: 00:00
  Data (56 bytes)
```

```
0000  00 b0 d0 5c 5b 55 00 b0 d0 5c 5a bd 08 00 45 00  ...\[U...\Z...E.
0010  00 54 00 54 00 00 40 01 2e 40 c3 dd e2 2d c3 dd  .T.T..@..@...-..
0020  e2 2c 08 00 11 0b a6 00 00 00 5d 70 4d 40 9f 40  .,.....]pM@.@
0030  0c 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#.%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37                                               67
```

Et l'entete de la reponse (N.B. "Type: 0 (Echo (ping) reply)"):

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x190b (correct)
  Identifieur: 0xa600
  Sequence number: 00:00
  Data (56 bytes)
```

Que remarquez vous pour le champ Identifieur et le champ Séquence Number?

Le bon usage des champs “Identifier” et “Sequence Number” est spécifiée par l’Internet Control Message Protocol. Tandis que le champ “Identifier” devrait tre utilisé pour faire la différence entre plusieurs sessions (messages envoyées stations différentes), le champ “Séquence Number” permet de distinguer les différentes messages envoyées la mme station.

Donner l’algorithme de calcul des deux octets de Checksum

Au debut le valeur de Checksum est ZERO. On fait la somme par colonnes du 1’s complimént de tous les bits du paquets et prend le 1’scomplément du résultat.

Quels genres d’erreur peuvent/ne peuvent pas tre détectés?

Chaque erreur qui change la valeur de la somme est détectés par l’algorithme checksum, les autres ne le sont pas (par exemple, un échange de 1 et 0 à la dernière position de deux blocs).

3 Le protocole UDP

Nous avons lancé socklab sur les deux machines, et après nous avons créé des sockets UDP avec ”sock”. Apres nous avons demandé à émettre un paquet vers une machine avec ”sendto”, et nous avons reçu le paquet sur l’autre machine avec ”recvfrom”.

```
User Datagram Protocol, Src Port: 1048 (1048), Dst Port: 1052 (1052)
  Source port: 1048 (1048)
  Destination port: 1052 (1052)
  Length: 5008
  Checksum: 0xc0c2
Data (1472 bytes)
```

A quoi sert l’identificateur de socket

L’identificateur de socket est un numero qui permet d’identifier le socket

[16] [16] [16] [16]
Source Port Dest. Port Message Length Checksum

Le checksum est le "one's complement" de la sum des "one's complement" de tous les octets envoyés dans les entetes IP, UDP et les données.

Quelles sont les informations passés à IP par UDP?

UDP passe l'address source et l'address destination a IP, et aussi le data.

3.1 Les variantes

Demandez la réception avant l'émission des données

Machine A a reçu le message quand machine B l'a envoyé.

Envoyez plusieurs paquets avant de demander leur réception

Machine A a reçu les messages une après l'autre. Chaque fois que nous avons fait recvfrom Machine A a reçu un seul message.

Demandez d'envoyer un paquet sur chacune des machines puis demandez de lire le paquet envoyé par la station distante

Machines A et B ont reçu les messages correctes.

Notez ce qu'il se passe quand vous demandez à recevoir plus ou moins d'octets que la station distante en envoie

Quand nous avons demandé a recevoir moins d'octets le message a été coupé. Quand nous avons demandé a recevoir plus d'octets le message a été correcte.

Envoyez un paquet vers une machine que vous au préalable, débranchée du réseau.

Nous avons débranché une machine et observé ce qui s'est passé avec une troisieme machine. Le paquet etais envoyé par Machine B, mais après ca il etait perdu. Nous avons rébranché machine A, mais il n'a pas reçu le paquet.

Envoyez 6 paquets de 5000 octets puis essayez de les réceptionner
Machine B a envoyé les paquets, et après ca Machine A á essayé de les réceptionner. Machine A n'a pas reçu tous le data.

Envoyez un paquet UDP vers un port inexistant.

Nous avons reçu un message ICMP("Destination Unreachable") qui a contenu le paquet le paquet que nous avons envoyé.

3.2 Résumé sur le fonctionnement du protocole UDP

Le protocole UDP est assez similaire à la protocole IP, mais il ajoute des autres fonctions. Il permet de spécifier un port, donc plusieurs échanges UDP peuvent s'exécuter sur une seule machine. Il ajoute aussi le checksum qui permet de vérifier si un paquet est correcte. Si le paquet n'est pas correcte il n'est pas renvoyé. Il est assez facile à perdre data, si on ne demande pas un paquet avec la taille correcte.

4 TCP

Nous n'avons pas réussi à finir cette partie pendant le TP, donc nous sommes désolés de présenter rien.